Scientific & Technical Information Center
S T I C
USPTO

STIC Search Report
EIC 2100

STIC Database Tracking Number: 117248

TO: Kambiz Zand Location: ~~4B02~~ 4C10 Art Unit : 2132 Thursday, March 25, 2004 Case Serial Number: 09/623037	From: Carol Wong Location: EIC 2100 PK2-4B33 Phone: 305-9729 carol.wong@uspto.gov

Search Notes

Dear Examiner Zand,

Attached are the search results (from commercial databases) for your case.

Color tags mark the patents/articles which appear to be most relevant to the case. Pls review all documents, since untagged items might also be of interest. If you wish to order the complete text of any document, pls submit request(s) directly to the EIC2100 Reference Staff located in PK2-4B40.

Pls call if you have any questions or suggestions for additional terminology, or a different approach to searching the case. Finally, pls complete the attached Search Results Feedback Form, as the EIC/STIC is continually soliciting examiners' opinion of the search service.

Thanks,
Carol

```
File 348:EUROPEAN PATENTS 1978-2004/Mar W02
         (c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20040318,UT=20040311
         (c) 2004 WIPO/Univentio

Set     Items   Description
S1     201095   PIN OR PINS OR PID OR PIDS OR UIN OR UINS
S2      29455   (SEQUENCE? ? OR SERIES)(1N)(NUMERIC? OR NUMBER? ? OR NUMER-
             AL? ? OR ALPHANUMERIC?)
S3      18078   PASSWORD? OR PASSCODE? OR PASSKEY? OR PASSNUMBER? OR PASSV-
             ALUE?
S4       1305   PASS()(WORD? ? OR KEY? ? OR CODE? ? OR NUMBER? ? OR VALUE?
              ? OR IDENTIFIER? OR ID OR SEQUENCE?)
S5      39867   (ID OR IDENTIFY? OR IDENTIFICATION? OR IDENTIFIE? ? OR AUT-
             HENTICAT? OR ACCESS OR AUTHORIZ? OR AUTHORIS?)()(CODE? ? OR N-
             UMBER? ? OR SEQUENCE)
S6          1   COENCYPHER? OR COENCIPHER? OR COCYPHER? OR COCIPHER? OR CO-
             ENCRYPT? OR COINCOD? OR COENCOD?
S7       1028   CO()(ENCIPHER? OR ENCYPHER? OR ENCOD??? ? OR INCOD??? ? OR
             ENCRYPT?)
S8     297149   VARIABLE? ?
S9      10736   S8(3N)(ADD OR ADDS OR ADDED OR ADDING OR ADDITIONAL OR SUP-
             PLEMENT? OR EXTRA OR AUXILIAR? OR ANCILL? OR ANOTHER OR AUGME-
             NT?)
S10     95900   (PARAMETER? OR PARAMETRE? OR VALUE OR VALUES OR NUMBER? ? -
             OR NUMERIC? OR NUMERAL? OR ALPHANUMERIC?)(2N)(CHANGEAB? OR CH-
             ANG??? ? OR VARY? OR VARIE? ? OR INCONSTAN? OR INDETERMINAT?)
S11      6195   (PARAMETER? OR PARAMETRE? OR VALUE OR VALUES OR NUMBER? ? -
             OR NUMERIC? OR NUMERAL? OR ALPHANUMERIC?)(2N)(UNFIX?? ? OR DY-
             NAMIC?)
S12      1949   S10:S11(3N)(ADD OR ADDS OR ADDED OR ADDING OR ADDITIONAL OR
              SUPPLEMENT? OR EXTRA OR AUXILIAR? OR ANCILL? OR ANOTHER OR A-
             UGMENT?)
S13      5429   (FURTHER OR SECOND OR PAIR?? ?)(1W)S8
S14       174   S1:S5(25N)(S6:S7 OR S9 OR S12)
S15      1752   S1:S5(25N)S10:S11
S16        61   S1:S5(25N)S13
S17         0   S14/TI,AB
S18        21   S14/TI,AB,CM
S19        26   S16/TI,AB,CM
S20      6137   IC='H04L-009'
S21      2076   IC='G06F-015/00'
S22       256   IC='G09C-001'
S23      2669   IC='H04M-003/42'
S24      1579   IC='H04M-015'
S25       111   S14:S16 AND S20:S24
S26        63   S14:S16 AND (S20 OR S22)
S27       109   S1:S5(10N)(S6:S7 OR S9 OR S12)
S28      1234   S1:S5(10N)S10:S11
S29        38   S1:S5(10N)S13
S30        48   S27:S29 AND (S20 OR S22)
S31        14   S27/TI,AB,CM
S32        17   S29/TI,AB,CM
S33        21   S27(25N)(ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR ENCOD???? ?
             OR INCOD???? ?)
S34        77   S28(25N)(ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR ENCOD???? ?
             OR INCOD???? ?)
S35         3   S29(25N)(ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR ENCOD???? ?
             OR INCOD???? ?)
S36        12   S34/TI,AB,CM
```

```
S37       102   S30:S33 OR S35:S36

 37/5,K/1     (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01605139
RC4 for packet encryption method
RC4 Verfahren zur Verschlusselung von Paketen
Methode RC4 pour le cryptage de paquets
PATENT ASSIGNEE:
  Avaya Technology Corp., (3148500), 211 Mount Airy Road, Basking Ridge, NJ
    07920, (US), (Applicant designated States: all)
INVENTOR:
  Garstin, Mark, 1137 Upper River Court, Mississauga, Ontario L5W 1C2, (CA)
  Gilman, Robert R., 3243 West 11th Avenue, Broomfield, Colorado 80020,
    (US)
  Wutzke, Mark, 7/52 Tranmere Street, Drummoye, New South Wales, (AU)
  Robinson, Richard L., 13920 Dogleg Lane, Broomfield, Colorado 80020, (US)
  Siddiqui, Anwar, 160 Claremont Avenue, No 6A, New York, New York 10027,
    (US)
LEGAL REPRESENTATIVE:
  Williams, David John et al (86433), Page White & Farrer, 54 Doughty
    Street, London WC1N 2LS, (GB)
PATENT (CC, No, Kind, Date):  EP 1326367  A1  030709 (Basic)
APPLICATION (CC, No, Date):   EP 2003250042 030103;
PRIORITY (CC, No, Date): US 38295 020104
DESIGNATED STATES: AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES; FI; FR; GB; GR;
  HU; IE; IT; LI; LU; MC; NL; PT; SE; SI; SK; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO
INTERNATIONAL PATENT CLASS:  H04L-009/12 ;  H04L-009/00

ABSTRACT EP 1326367 A1
    The present efficient packet encryption method decreases the
  computation time to encrypt and decrypt successive packets of plaintext
  data. An S-vector is generated and the S-vector is used to encrypt
  successive packets of plaintext, thus reducing the per packet
  encryption/decryption time. The formula for encrypting successive packets
  includes use of the packet sequence number with a third variable injected
  to eliminate the predictability of the variables, thus making the present
  efficient packet encryption method more secure. A fourth variable is
  injected into the calculations to generate an encryption stream that does
  not repeat as frequently to provide additional security from hackers. For
  encrypting a packet having a long payload of plaintext, a packet byte
  sequence number is used to generate an encryption stream that is less
  likely to repeat within a particular packet.
ABSTRACT WORD COUNT: 134
NOTE:
  Figure number on first page: 3

LEGAL STATUS (Type, Pub Date, Kind, Text):
 Application:     030709 A1 Published application with search report
 Examination:     031126 A1 Date of request for examination: 20030926
 Examination:     031217 A1 Date of dispatch of the first examination
                            report: 20031104
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text  Language    Update    Word Count
      CLAIMS A  (English)  200328      1335
      SPEC A    (English)  200328      5282
Total word count - document A          6617
```

Total word count - document B 0
Total word count - documents A + B 6617

INTERNATIONAL PATENT CLASS: **H04L-009/12** ...

... **H04L-009/00**

...CLAIMS part and a second part;
setting a first variable as the first part of the **sequence number** ;
setting a **second variable** as the second part of the **sequence number** ;
setting a byte **sequence** number;
calculating a third variable as the sum of the second variable plus the byte **sequence number** ;
incrementing the byte **sequence number** by one;
calculating a fourth **variable** by **adding** the first **variable** plus the value within the S-vector pointed to by the third variable;
locating an **encryption** byte, wherein the location of the **encryption** byte within the S-vector is pointed to by the sum of the value within ...

...at least one byte of ciphertext.
2. The method of claim 1 where setting a **second variable** further comprises:
exclusive ORing the second part of the **sequence number** and the value within the S-vector pointed to by the first variable.
3. The...

...portion and a second portion;

setting a first variable using the first portion of the **sequence** number;

setting a second variable using the second portion of the sequence number; and

setting...

...of the plurality of bytes of plaintext, calculating a next encryption byte, the calculating comprising:
adding the second **variable** to the byte **sequence number** to produce a third variable;
calculating a fourth **variable** by **adding** the first **variable** plus the value within the S-vector pointed to by the third variable;
locating a next **encryption** byte within the S-vector by adding the values within the S-vector pointed to...

...the third variable and the fourth variable to calculate a pointer to locate the next **encryption** byte; setting the **second variable** equal to the third variable; and incrementing the byte **sequence number** by one.
5. The method of claim 4 wherein calculating a **second variable** comprises:
exclusive ORing the second portion of the **sequence number** with the value within the S-vector pointed to by the first variable.
6. The...

...the sequence number;
setting a first variable j according to j = first part of the **sequence number** ;

calculating a **second variable** i according to i = second part of the **sequence number** ;
for each successive byte of the plurality of bytes of plaintext P, calculating a next...or more packets to a receiver.
12. The method of claim 11 wherein calculating a **second variable** i further comprises:
exclusive ORing the low order **sequence number** and the value within the S-vector pointed to by first variable according to i...

...each successive byte of the plurality of bytes of plaintext P, calculating a next successive **encryption** byte E, the calculating comprising:
setting a first variable j according to j = high order of the **sequence number** ;
calculating a **second variable** i according to i = (low order of the **sequence number**) (plus sign in circle) S(j);
setting a counter r;
further calculating the first variable...

37/5,K/2 (Item 2 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01513206
ENCRYPTING DEVICE
VERSCHLUSSELUNGSEINRICHTUNG
DISPOSITIF DE CHIFFREMENT
PATENT ASSIGNEE:
MITSUBISHI DENKI KABUSHIKI KAISHA, (208589), 2-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo 100-8310, (JP), (Applicant designated States: all)
INVENTOR:
KASUYA, Tomomi, c/o Mitsubishi Denki Kabushiki K., 2-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo 100-8310, (JP)
CHIKAZAWA, Takeshi, c/o Mitsubishi Denki K. K., 2-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo 100-8310, (JP)
WAKABAYASHI, Takao, c/o Mitsubishi Denki K. K., 2-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo 100-8310, (JP)
UGA, Shinsuke, c/o Mitsubishi Denki Kabushiki K., 2-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo 100-8310, (JP)
LEGAL REPRESENTATIVE:
Pfenning, Meinig & Partner (100961), Mozartstrasse 17, 80336 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1376922 A1 040102 (Basic)
WO 2002082715 021017
APPLICATION (CC, No, Date): EP 2001917799 010403; WO 2001JP2880 010403
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: **H04L-009/00 ; G09C-001/00**

ABSTRACT EP 1376922 A1
A random number sequence is previously generated by the function f8 for data confidentiality processing, which generates a random number sequence, and stored in a random number sequence memory (buffer). When data (message) is input, the random number sequence stored in the random number sequence memory is obtained, and the data (message) is encrypted by an XOR circuit to generate ciphertext data. In case of decrypting data, a random number sequence is also previously generated by the function f8 for data confidentiality processing and stored in the random

```
  number sequence memory (buffer). When the ciphertext data is input, by
  the XOR circuit, the random number sequence stored in the random number
  sequence memory is read and the ciphertext data is decrypted into the
  data (message).
ABSTRACT WORD COUNT: 126
NOTE:
  Figure number on first page: 25

LEGAL STATUS (Type, Pub Date, Kind, Text):
 Application:     021211 A1 International application. (Art. 158(1))
 Application:     021211 A1 International application entering European
                            phase
 Application:     040102 A1 Published application with search report
 Examination:     040102 A1 Date of request for examination: 20030925
LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:
Available Text  Language   Update    Word Count
      CLAIMS A  (English)  200401     1804
      SPEC A    (English)  200401    13439
Total word count - document A        15243
Total word count - document B            0
Total word count - documents A + B   15243

INTERNATIONAL PATENT CLASS:  H04L-009/00 ...

... G09C-001/00


 37/5,K/9     (Item 9 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01334062
Method for activating an encrypted file
Verfahren zur Freischaltung einer verschlusselten Datei
Procede pour activer un fichier de donnees cryptees
PATENT ASSIGNEE:
  Mannesmann VDO Aktiengesellschaft, (205194), Kruppstrasse 105, 60388
    Frankfurt am Main, (DE), (Applicant designated States: all)
INVENTOR:
  Thoone, Martin, Kirchstrasse 21, D-35614 Asslar, (DE)
  Drijfhout, Theo, Geheimrat-Gester-Strasse 2, D-35619 Braunfels, (DE)
LEGAL REPRESENTATIVE:
  Rassler, Andrea, Dipl.-Phys. (65972), Kruppstrasse 105, 60388 Frankfurt,
    (DE)
PATENT (CC, No, Kind, Date):  EP 1139196  A1  011004 (Basic)
APPLICATION (CC, No, Date):   EP 2000106809 000330;
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI;
  LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: G06F-001/00

ABSTRACT EP 1139196 A1 (Translated)
    Releasing a coded data file involves the use of equipment identifiers
  established by using enciphered codes and keys passed between a local
  computer system and a central station
    The method involves passing an equipment identifier from a local
  computer system to a central station, computing a new equipment
  identifier using a change code, specifying a first enciphered code using
  a key, specifying a second enciphered code using the data file
  identifier, passing the enciphered codes to the local system, computing
```

the new equipment identifier, the key and data file identifier in the local system and releasing the data file.

The method involves passing an equipment identifier (ID(i-1)) from a local computer system to a central station, computing a new equipment identifier (ID(i)) from the equipment **number** and a **change** code, specifying a first **enciphered** code (**PIN**) using the computed code and a key (k), specifying a second **enciphered** code (ACW) using the data file identifier and the key, passing the **enciphered** codes to the local system, computing the new equipment identifier in the local system from the stored identifier and the change code, computing the key from the first enciphered code and the equipment identifier, computing the data file identifier (AC) from the second enciphered code and the key and releasing the data file for use by the local system. Independent claims are also included for the following: a system for managing and releasing access rights to data files.

TRANSLATED ABSTRACT WORD COUNT: 239

ABSTRACT EP 1139196 A1

Es wird ein Verfahren zur Freigabe von Nutzungsrechten an einer auf einem Speichermedium zusammen mit mindestens einer weiteren Datei abgespeicherten und mit einer Kennung versehenen Datei zur Nutzung durch ein einziges oder eine begrenzte Anzahl von lokalen Computersystemen beschrieben.

Hierzu wird von einer Zentralstelle ein erster und ein zweiter chiffrierter Code PIN bzw. ACW berechnet, der einen Schlussel k zur Entschlusselung der verschlusselt abgespeicherten Dateien und eine Geratekennzahl ID enthalt. Die Geratekennzahl ID wird bei jeder neuen Freigabe geandert. Nach Eingabe der beiden chiffrierten Codes in das Computersystem wird in diesem zunachst eine neue Geratekennzahl ID aus abgespeicherten Daten und mit dieser neuen Geratekennzahl ID und dem ersten chiffrierten Code PIN des Schlussel k und mit dem Schlussel k und dem zweiten chiffrierten Code ACW eine Kennung AC der freizuschaltenden Datei berechnet.

ABSTRACT WORD COUNT: 133

NOTE:

Figure number on first page: 5

```
LEGAL STATUS (Type, Pub Date, Kind, Text):
 Application:     011004 A1 Published application with search report
 Assignee:        020109 A1 Transfer of rights to new applicant: Siemens
                            Aktiengesellschaft (3937630) Wittelsbacherplatz
                            2 80333 Munchen DE
 Examination:     020116 A1 Date of request for examination: 20011119
 Deleted:         020515 A1 Legal representative(s) deleted 20020325
LANGUAGE (Publication,Procedural,Application): German; German; German
FULLTEXT AVAILABILITY:
Available Text  Language   Update    Word Count
      CLAIMS A   (German)  200140       980
      SPEC A     (German)  200140      4134
Total word count - document A          5114
Total word count - document B             0
Total word count - documents A + B     5114
```

...ABSTRACT system to a central station, computing a new equipment identifier (ID(i)) from the equipment **number** and a **change** code, specifying a first **enciphered** code (**PIN**) using the computed code and a key (k), specifying a second **enciphered** code (ACW) using the data file identifier and the key, passing the **enciphered** codes to the local system, computing the new equipment identifier in the local system from ...

```
 37/5,K/13     (Item 13 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01008069
METHOD OF TRANSMITTING VARIABLE-LENGTH FRAME, TRANSMITTER, AND RECEIVER
VERFAHREN,  SENDER  UND  EMPFANGER ZUR UBERTRAGUNG VON RAHMEN MIT VARIABLER
    LANGE
PROCEDE DE TRANSMISSION DE TRAME A LONGUEUR VARIABLE, EMETTEUR ET RECEPTEUR
PATENT ASSIGNEE:
  NTT MOBILE COMMUNICATIONS NETWORK INC., (1560153), 10-1, Toranomon
    2-chome, Minato-ku, Tokyo 105-8436, (JP), (applicant designated states:
    DE;FR;GB;IT;SE)
INVENTOR:
  NAKA, Nobuhiko, B-202, 1-36-20, Ohoka, Minami-ku, Yokohama-shi, Kanagawa
    232-0061, (JP)
  KAWAHARA, Toshiro, 2-506, 2-1-3, Hayashi, Yokosuka-shi, Kanagawa 238-0315
    , (JP)
LEGAL REPRESENTATIVE:
  HOFFMANN - EITLE (101511), Patent- und Rechtsanwalte Arabellastrasse 4,
    81925 Munchen, (DE)
PATENT (CC, No, Kind, Date):  EP 915588  A1  990512 (Basic)
                              WO 9852315  981119
APPLICATION (CC, No, Date):   EP 98919605 980515;  WO 98JP2141  980515
PRIORITY (CC, No, Date): JP 97127608 970516
DESIGNATED STATES: DE; FR; GB; IT; SE
INTERNATIONAL PATENT CLASS: H04L-007/08; H04J-003/06;
CITED REFERENCES (WO A):
  SANAE HOTANI, TOSHIO MIKI, "Study on Variable-Frame Synchronizing Method
    Suitable for MPEG-4 Audio (in Japanese)", TECHNICAL RESEARCH REPORT OF
    IEICE (DIGITAL SIGNAL PROCESSING), Vol. 96, No. 477, (DSP96-113), 23
    January 1997, pages 35-42.
  NOBUHIKO NAKA, TAKASHI SUZUKI, TOSHIRO KAWAHARA, TOSHIO MIKI, "Study on
    Protection of Variable-Frame Synchronization (in Japanese)", TECHNICAL
    RESEARCH REPORT OF IEICE (RADIO COMMUNICATION SYSTEM), Vol. 97, No.
    193, (RCS97-50), 24 July 1997, pages 23-28.;

ABSTRACT EP 915588 A1
    A variable length frame transmission method making it possible to
  accurately and easily establish synchronism at the receiver side without
  redundancy of system under an environment in which a code error easily
  occurs.
    In a transmitter, a variable length frame division section 1 divides a
  variable length frame f into code strings f1)) and f2)) having a length
  ratio of 1:1. A first synchronization flag addition section 3-1 adds a
  synchronization flag S1)) to the head of the code string f1)) and a
  second synchronization flag addition section 3-2 adds a synchronization
  flag S2)) to the head of the code string f2)). The synchronization flags
  have contents different from each other, but they have the same length.
  Code strings having synchronization flags are multiplexed by a changeover
  switch 4 and formed into a variable length frame. A series of variable
  length frames obtained from the changeover switch 4 are transmitted to a
  receiver as serial data. In the receiver, the start and end points of
  each frame is obtained based on the position of each synchronization flag
  in the serial data.
ABSTRACT WORD COUNT: 182

LEGAL STATUS (Type, Pub Date, Kind, Text):
 Application:      990407 A1 International application (Art. 158(1))
 Application:      990512 A1 Published application (A1with Search Report
                        ;A2without Search Report)
 Change:          990526 A1 Title of invention (German) (change)
 Examination:     990811 A1 Date of request for examination: 19990115
LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:
Available Text  Language    Update    Word Count
      CLAIMS A  (English)  9922        1417
      SPEC A    (English)  9922       12770
Total word count - document A         14187
Total word count - document B             0
Total word count - documents A + B    14187

...CLAIMS flags.
  7. The variable length frame transmission method according to claim 6,
      wherein
   the transmitter  encodes  the additional information including the
      information concerned with the structure of the variable length frame
      to generate  identification  code  strings by encoding methods
      different between the consecutive  variable  length frames and  adds
      the  identification  code  strings after the synchronization flags
      to transmit the serial data, and
   the receiver detects the...


 37/5,K/14     (Item 14 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

00957049
System  and  method  for  authentication,  and  device  and  method  for
    autentication
System  und  Verfahren  zur Authentifikation, und Vorrichtung und Verfahren
    zur Authentifikation
Systeme   et   methode   d'authentification,   et   dispositif  et  methode
    d'authentification
PATENT ASSIGNEE:
  SONY CORPORATION, (214022), 7-35, Kitashinagawa 6-chome Shinagawa-ku,
    Tokyo, (JP), (Proprietor designated states: all)
INVENTOR:
  Kusakabe, Susumu, c/o Sony Corporation, 7-35, Kitashinagawa 6-chome,
    Shinagawa-ku, Tokyo, (JP)
  Takada, Masayuki, c/o Sony Corporation, 7-35, Kitashinagawa 6-chome,
    Shinagawa-ku, Tokyo, (JP)
  Ishibashi, Yoshihito, c/o Sony Corporation, 7-35, Kitashinagawa 6-chome,
    Shinagawa-ku, Tokyo, (JP)
LEGAL REPRESENTATIVE:
  Melzer, Wolfgang, Dipl.-Ing. et al (8278), Patentanwalte Mitscherlich &
    Partner, Sonnenstrasse 33, 80331 Munchen, (DE)
PATENT (CC, No, Kind, Date):  EP 867843  A2  980930 (Basic)
                              EP 867843  A3  000920
                              EP 867843  B1  040121
APPLICATION (CC, No, Date):   EP 98105233 980323;
PRIORITY (CC, No, Date): JP 9773205 970326; JP 97110889 970428
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
RELATED DIVISIONAL NUMBER(S) - PN (AN):
  EP 1339028  (EP 2003000440)
INTERNATIONAL PATENT CLASS: G07F-007/10;  H04L-009/00 ;  H04L-009/08
CITED PATENTS (EP B): EP 422230 A; EP 427465 A; EP 552392 A; US 5293029 A
CITED REFERENCES (EP B):
```

PATENT ABSTRACTS OF JAPAN vol. 1997, no. 03, 31 March 1997 (1997-03-31) & JP 08 305662 A (FUJITSU LTD), 22 November 1996 (1996-11-22);

ABSTRACT EP 867843 A2

In authentication using a plurality of cipher keys, the authentication time is shortened. In the case that an encipher key to encipher key are required to take an access to each area out of the area to area in a memory of an IC card, a plurality of areas to have an access is informed to the IC card from a reader writer, a plurality of cipher keys corresponding to these areas (for example, cipher key 1, cipher key 2, and cipher key 4) is read out, and reduction processing section generates one reduction key from these cipher keys. A random number which is generated from a random number generation section of the reader writer is transferred to the IC card, and an encipherment section enciphers the random number using the reduction key. The reader writer receives the enciphered random number from the IC card, and deciphers it using the reduction key, and judges the IC card to be proper if the deciphered random number is equal to the generated random number.

ABSTRACT WORD COUNT: 173

NOTE:
Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):

Change:	000920	A2	International Patent Classification changed: 20000801
Application:	980930	A2	Published application (A1with Search Report ;A2without Search Report)
Grant:	040121	B1	Granted patent
Change:	030305	A2	Application number of divisional application (Article 76) changed: 20030114
Search Report:	000920	A3	Separate publication of the search report
Examination:	010502	A2	Date of request for examination: 20010308
Examination:	020130	A2	Date of dispatch of the first examination report: 20011217
Change:	040107	A2	Title of invention (German) changed: 20031120

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	199840	2573
CLAIMS B	(English)	200404	753
CLAIMS B	(German)	200404	716
CLAIMS B	(French)	200404	807
SPEC A	(English)	199840	9076
SPEC B	(English)	200404	7086
Total word count - document A			11651
Total word count - document B			9362
Total word count - documents A + B			21013

...INTERNATIONAL PATENT CLASS: **H04L-009/00** ...

... **H04L-009/08**

...SPECIFICATION first communication means of the first device using the first key corresponding to the key **identification number** , and a **changing** means (for example, a control section 36 shown in Fig. 18) for judging whether the...

...CLAIMS claim 15, wherein said second device comprises:
the second decipherment means for deciphering said first **enciphered** data and second **enciphered** data received from said first communication means of said first device using said first key

corresponding to said key **identification** **number** ; and
changing means for determining whether said second key and third key are in a prescribed relation...

37/5,K/16 (Item 16 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00899156
Cryptographic unit touch point logic
Verschlusselungseinheit mit Kontaktpunktlogik
Organe cryptographique avec logique de point de contact
PATENT ASSIGNEE:
Cheyenne Property Trust, (2740010), 425 California Street, Suite 1450, San Francisco, CA 94104, (US), (Proprietor designated states: all)
INVENTOR:
Klemba, Keith, 3319 Vernon Terrace, Palo Alto, CA 94303, (US)
Merkling, Roger, 3143 Stockton Place, Palo Alto, CA 94303, (US)
LEGAL REPRESENTATIVE:
Schoppe, Fritz, Dipl.-Ing. (55463), Schoppe, Zimmermann, Stockeler & Zinkler Patentanwalte Postfach 71 08 67, 81458 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 821508 A2 980128 (Basic)
EP 821508 A3 980506
EP 821508 B1 030409
APPLICATION (CC, No, Date): EP 97110865 970701;
PRIORITY (CC, No, Date): US 685076 960723
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: G06F-001/00; **H04L-009/32** ; H04L-029/06
CITED PATENTS (EP B): WO 95/14338 A; US 4649510 A; US 5164988 A
CITED REFERENCES (EP B):
CONNER D: "RECONFIGURABLE LOGIC" EDN ELECTRICAL DESIGN NEWS, vol. 41, no. 7, 28 March 1996, pages 53-56, 58, 60, 62 - 64, XP000592126
FERREIRA R: "THE PRACTICAL APPLICATION OF STATE OF THE ART SECURITY IN REAL ENVIRONMENTS" ADVANCES IN CRYPTOLOGY - AUSCRYPT '90, 8 January 1990, pages 334-355, XP000145211
WOO T Y C ET AL: "AUTHENTICATION FOR DISTRIBUTED SYSTEMS" COMPUTER, vol. 25, no. 1, 1 January 1992, pages 39-52, XP000287833;

ABSTRACT EP 821508 A2

Cryptographic hardware is provided that is disabled at the time of shipment and that is selectively enabled in a trusted fashion using methods and interfaces that may be controlled by and governed by government policy in strict compliance with existing and future legislation. A given cryptographic algorithm is disabled/enabled at several points, referred to as Touch Points, and referred to collectively as Touch Point Logic. Because attributes of each touch point are satisfied by providing data that are referred to as Touch Point Data, manufactures are allowed to include disabled cryptographic hardware in their products and governments are provided with the ability to enable this cryptographic hardware only in compliance with governing legislation.

ABSTRACT WORD COUNT: 114
NOTE:
Figure number on first page: 3

LEGAL STATUS (Type, Pub Date, Kind, Text):
Examination: 010131 A2 Date of dispatch of the first examination report: 20001215
Application: 980128 A2 Published application (A1with Search Report ;A2without Search Report)

```
 Grant:            030409 B1 Granted patent
 Search Report:    980506 A3 Separate publication of the European or
                             International search report
 Change:           980506 A2 International patent classification (change)
 Change:           980506 A2 Obligatory supplementary classification
                             (change)
 Examination:      981223 A2 Date of filing of request for examination:
                             981022
 Change:           990120 A2 Designated Contracting States (change)
 Assignee:         990922 A2 Transfer of rights to new applicant: Cheyenne
                             Property Trust (2740010) 425 California Street,
                             Suite 1450 San Francisco, CA 94104 US
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text  Language   Update    Word Count
      CLAIMS A  (English)  199805       611
      CLAIMS B  (English)  200315      759
      CLAIMS B   (German)  200315      771
      CLAIMS B   (French)  200315      842
      SPEC A    (English)  199805       7887
      SPEC B    (English)  200315     8241
Total word count - document A         8501
Total word count - document B        10613
Total word count - documents A + B   19114

...INTERNATIONAL PATENT CLASS:  H04L-009/32

...SPECIFICATION but does not really trust the cryptographic unit. Every
  now and then the policy may change the sequence  number . Thus, the
  policy may normally increment the sequence  number  one by one by one,
  and then every now and then it issues another random...

...SPECIFICATION but does not really trust the cryptographic unit. Every
  now and then the policy may change the sequence  number . Thus, the
  policy may normally increment the sequence  number  one by one by one,
  and then every now and then it issues another random...


 37/5,K/17     (Item 17 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

00893799
Authentication method, communication method, and information processing
    apparatus
Authentifizierungsverfahren, Kommunikationsverfahren und Informationsverarb
    eitungseinrichtung
Procede d'authentification, procede de communication et dispositif de
    traitement d'information
PATENT ASSIGNEE:
  SONY CORPORATION, (214022), 7-35, Kitashinagawa 6-chome Shinagawa-ku,
    Tokyo, (JP), (Applicant designated States: all)
INVENTOR:
  Kusakabe, Susumu, c/o Sony Corporation, 7-35, Kitashinagawa 6-chome,
    Shinagawa-ku, Tokyo, (JP)
  Takada, Masayuki, c/o Sony Corporation, 7-35, Kitashinagawa 6-chome,
    Shinagawa-ku, Tokyo, (JP)
LEGAL REPRESENTATIVE:
  Nicholls, Michael John et al (61941), J.A. KEMP & CO. 14, South Square
    Gray's Inn, London WC1R 5JJ, (GB)
```

PATENT (CC, No, Kind, Date): EP 817420 A2 980107 (Basic)
EP 817420 A3 020515
APPLICATION (CC, No, Date): EP 97304682 970627;
PRIORITY (CC, No, Date): JP 96168965 960628
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: **H04L-009/32** ; G07F-007/10

ABSTRACT EP 817420 A2

Mutual authentication is performed. A reader/writer (R/W) transmits to an IC card a code C1 such that a random number RA is encrypted using a key KB. The IC card decrypts the code C1 into plain text M1 using the key KB. The IC card transmits to the R/W a code C2 such that the plain text M1 is encrypted using a key KA and a code C3 such that a random number RB is encrypted using the key KA. The R/W decrypts the codes C2 and C3 into plain text M2 and plain text M3, respectively, using the key KA. When the R/W determines that the plain text M2 and the random number RA are the same, it authenticates the IC card. Next, the R/W transmits to the IC card a code C4 such that the plain text M3 is encrypted using the key KB. The IC card decrypts the code C4 into plain text M4 using the key KB. When the IC card determines that the plain text M4 and the random number RB are the same, it authenticates the R/W.

ABSTRACT WORD COUNT: 184
NOTE:
Figure number on first page: 1
LEGAL STATUS (Type, Pub Date, Kind, Text):

Change:	020515	A2	International Patent Classification changed: 20020326
Application:	980107	A2	Published application (A1with Search Report ;A2without Search Report)
Examination:	030205	A2	Date of dispatch of the first examination report: 20021220
Search Report:	020515	A3	Separate publication of the search report
Examination:	021218	A2	Date of request for examination: 20021018

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9802	2433
SPEC A	(English)	9802	7571
Total word count - document A			10004
Total word count - document B			0
Total word count - documents A + B			10004

INTERNATIONAL PATENT CLASS: **H04L-009/32** ...

...CLAIMS identification number.

18. An information processing apparatus according to claim 16 or 17, wherein said **identification number** is **changed** for each **encryption** of said first command.
19. An information processing apparatus according to claim 18, wherein said identification number is increased for each **encryption** of said first command.
20. An information processing apparatus according to claim 17, 18 or... with said eighth code.
27. An information processing apparatus according to claim 26, wherein said **identification number** is **changed** for each **encryption** of said seventh code.
28. An information processing apparatus according to claim 27, wherein said identification number is increased for each **encryption** of said seventh code.
29. An information processing apparatus according to any one of claims...

```
 37/5,K/18     (Item 18 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

00891835
FUNCTION ACCESS CONTROL SYSTEM COMPRISING A CLOCK SYNCHRONISATION DEVICE
EINE UHRSYNCHRONISIERUNGSVORRICHTUNG ENTHALTENDES ZUGANGSKONTROLLSYSTEM ZU
    EINER FUNKTION
SYSTEME DE CONTROLE D'ACCES A UNE FONCTION COMPORTANT UN DISPOSITIF DE
    SYNCHRONISATION D'HORLOGES
PATENT ASSIGNEE:
  ACTIVCARD, (1446992), 24-28, avenue du General-de-Gaulle, 92156 Suresnes
    Cedex, (FR), (Proprietor designated states: all)
INVENTOR:
  AUDEBERT, Yves, 237, Forrester Road, LOS GATOS, CA 95032, (US)
LEGAL REPRESENTATIVE:
  Colas, Jean-Pierre (14815), Cabinet JP Colas 37, avenue Franklin D.
    Roosevelt, 75008 Paris, (FR)
PATENT (CC, No, Kind, Date):  EP 891610  A1  990120 (Basic)
                              EP 891610  B1  020529
                              WO 9736263  971002
APPLICATION (CC, No, Date):   EP 97915536 970321;  WO 97FR504  970321
PRIORITY (CC, No, Date): US 620162 960322; FR 964797 960417
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; NL;
  PT; SE
INTERNATIONAL PATENT CLASS: G07F-007/10; E05B-049/00
CITED PATENTS (EP B): EP 215291 A; EP 419306 A; EP 698706 A; DE 4223258 A
NOTE:
  No A-document published by EPO
LEGAL STATUS (Type, Pub Date, Kind, Text):
 Examination:      010404 A1 Date of dispatch of the first examination
                             report: 20010215
 Application:      971229 A1 International application (Art. 158(1))
 Oppn None:        030521 B1 No opposition filed: 20030303
 Change:           020417 A1 Inventor information changed: 20020226
 Grant:            020529 B1 Granted patent
 Application:      990120 A1 Published application (A1with Search Report
                             ;A2without Search Report)
 Examination:      990120 A1 Date of filing of request for examination:
                             980929
LANGUAGE (Publication,Procedural,Application): French; French; French
FULLTEXT AVAILABILITY:
Available Text  Language   Update    Word Count
      CLAIMS B  (English)  200222     2366
      CLAIMS B   (German)  200222     2404
      CLAIMS B   (French)  200222     2392
      SPEC B     (French)  200222     8281
Total word count - document A           0
Total word count - document B        15443
Total word count - documents A + B   15443

...CLAIMS third calculating means (79, 81 to 84 ; 57, 58, 60, 61) for
   c) retaining as second variable (Tc ; Nc) for the calculation of
      said second password (Aa) said substituted variable, if said
      substituted variable and said current value (Ta ; Na) of...

...adjusting generating a substituted and adjusted variable (Tc1, Tc2, Tc3;
      Nc1), and
   e) retaining as second variable (Tc, Nc) for the calculation of said
```

second **password** (Aa) said substituted and adjusted variable.
2. System according to claim 1, characterized in that...

37/5,K/19 (Item 19 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00882574
Client/server protocol for proving authenticity
Kunden/Server-Protokoll zum Uberprufen der Echtheit
Protocol client/serveur pour demontrer leur authenticite

PATENT ASSIGNEE:
RSA Data Security, Inc., (2317770), 100 Marine Parkway, Redwood City, California 94065-1031, (US), (applicant designated states: AT;BE;CH;DE;DK;ES;FI;FR;GB;GR;IE;IT;LI;LU;MC;NL;PT;SE)

INVENTOR:
Kaliski, Burton S., Jr., 474 Emerald Avenue, San Carlos, California 94070 , (US)

LEGAL REPRESENTATIVE:
Allman, Peter John et al (27675), MARKS & CLERK, Sussex House, 83-85 Mosley Street, Manchester M2 3LG, (GB)

PATENT (CC, No, Kind, Date): EP 807911 A2 971119 (Basic)
EP 807911 A3 990707
APPLICATION (CC, No, Date): EP 97303229 970512;
PRIORITY (CC, No, Date): US 648442 960515; US 845196 970421
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
INTERNATIONAL PATENT CLASS: G07F-019/00; G06F-017/60; **H04L-009/**32 ; G07F-007/10

ABSTRACT EP 807911 A2

A protocol for establishing the authenticity of a client to a server in an electronic transaction by encrypting a certificate with a key known only to the client and the server. The trust of the server, if necessary, can be established by a public key protocol. The client generates and sends over a communications channel a message containing at least a part of a certificate encrypted with the server's public key or a secret session key. The server receives and processes the message to recover at least part of the certificate, verifies and accepts it as proof of the client's authenticity.

ABSTRACT WORD COUNT: 102

LEGAL STATUS (Type, Pub Date, Kind, Text):

Assignee:	011017	A2	Transfer of rights to new applicant: RSA Security Inc, (3855710) 100 Marine Parkway Redwood City, California 94065-1031 US
Examination:	20000308	A2	Date of request for examination: 20000106
Withdrawal:	020904	A2	Date application deemed withdrawn: 20020227
Examination:	011128	A2	Date of dispatch of the first examination report: 20011016
Application:	971119	A2	Published application (A1with Search Report ;A2without Search Report)
Search Report:	990707	A3	Separate publication of the European or International search report
Change:	990707	A2	Obligatory supplementary classification (change)

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9711W2	4394

```
     SPEC A    (English)  9711W2      8944
Total word count - document A        13338
Total word count - document B            0
Total word count - documents A + B   13338
```

...INTERNATIONAL PATENT CLASS: **H04L-009/32**

...SPECIFICATION program to be executed by processor 2, clock 8 is set (or an initial time- **varying value** , e.g., a **sequence number** or a timestamp is set in one of the memories when a clock is not...

37/5,K/20 (Item 20 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00870002
Identification number issuing device and identification number verification device
Ausweisszahlausgabegerat und Ausweisszahluberprufungsgerat
Dispositif pour la creation de numeros d'identification et dispositif de verification de numeros d'identification

PATENT ASSIGNEE:
MITSUBISHI DENKI KABUSHIKI KAISHA, (208580), 2-3, Marunouchi 2-chome Chiyoda-ku, Tokyo 100, (JP), (Applicant designated States: all)

INVENTOR:
Yoshida, Hideo, c/o Mitsubishi Denki K.K., 2-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo 100, (JP)
Nakamura, Takahiko, c/o Mitsubishi Denki K.K., 2-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo 100, (JP)
Nishikawa, Keiichi, c/o Mitsubishi Denki K.K., 2-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo 100, (JP)

LEGAL REPRESENTATIVE:
Pfenning, Meinig & Partner (100961), Mozartstrasse 17, 80336 Munchen, (DE)

```
PATENT (CC, No, Kind, Date):  EP 798891  A2  971001 (Basic)
                              EP 798891  A3  000927
APPLICATION (CC, No, Date):   EP 96118366 961115;
PRIORITY (CC, No, Date): JP 9676884 960329
DESIGNATED STATES: DE; FR; NL
```

INTERNATIONAL PATENT CLASS: **H04L-009/32** ; H03M-013/00; H03M-005/00; G06F-007/10

ABSTRACT EP 798891 A2

An identification number issuing device comprising a code converter portion for converting an identification number character string constructed of character string of alphabets, numerals and the like into codes having one-to-one correspondence to letters (characters), and a check and selection portion for selecting as an identification number the character string corresponding to the code string that is determined to meet the Reed-Solomon code rule with the code being a symbol and the string of the symbol being a code length. The identification number is issued based on the Reed-Solomon code of a generating polynomial having a plurality of initial elements as roots, and for additional issuing, identification numbers are additionally issued based on the Reed-Solomon code with the number of elements of the generating polynomial reduced by 1.

ABSTRACT WORD COUNT: 129

NOTE:
Figure number on first page: NONE

```
LEGAL STATUS (Type, Pub Date, Kind, Text):
 Change:           000927 A2 International Patent Classification changed:
                             20000809
 Application:      971001 A2 Published application (A1with Search Report
                             ;A2without Search Report)
 Examination:      001206 A2 Date of request for examination: 20001012
 Search Report:    000927 A3 Separate publication of the search report
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text  Language   Update    Word Count
      CLAIMS A  (English)  9709W4      629
      SPEC A    (English)  9709W4     4445
Total word count - document A         5074
Total word count - document B            0
Total word count - documents A + B    5074

INTERNATIONAL PATENT CLASS:  H04L-009/32 ...

...SPECIFICATION the length of the identification number and without making
  the user aware of the additional  identification   number , and further,
  error detection and correction capability of the  identification   number
   is  varied  in accordance with the system.
    According to an eighth aspect of the present invention, the...


 37/5,K/27     (Item 27 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

00438533
Telephone  arrangement  for  remote loading of telephonic subscription data
    from an autonomous station.
Telefonanlage   fur   das   Fernladen   von   Fernsprechabonnement-Daten   einer
    autonomen Station.
Installation   telephonique   pour   le   chargement   a   distance   de   donnees
    d'abonnement telephonique d'une station autonome.
PATENT ASSIGNEE:
  FRANCE TELECOM, (1334140), 6, Place d'Alleray, F-75015 Paris, (FR),
    (applicant designated states: DE;FR;GB)
INVENTOR:
  Langrand, Franck, 19, rue Buot, F-75013 Paris, (FR)
  Mazziotto, Gerald, 56, rue du Moulin Vert, F-75014 Paris, (FR)
  Baudoux, Sophie, 32, rue des Cordelieres, F-75013 Paris, (FR)
LEGAL REPRESENTATIVE:
  Placais, Jean-Yves et al (17891), Cabinet Netter, 40, rue Vignon, F-75009
    Paris, (FR)
PATENT (CC, No, Kind, Date):  EP 459065  A1  911204 (Basic)
                              EP 459065  B1  950405
APPLICATION (CC, No, Date):   EP 90401664 900614;
PRIORITY (CC, No, Date): FR 906662 900529
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: H04Q-007/20;
CITED REFERENCES (EP A):
  ELECTRICAL COMMUNICATION vol. 63, no. 4, 1989, BRUSSELS (BE) pages 389 -
    399; M.BALLARD ET AL: 'Cellular Mobile Radio as an Intelligent Network
    Application '
  PREMIER COLLOQUE INTERNATIONAL SUR L'INTELLIGENCE DANS LES RESEAUX Mars
    1989, BORDEAUX (FR) pages 57 - 61; J.A. AUDESTAND: 'Intelligence in
    public land mobile networks: use of the mobile application part '
```

PROCEEDINGS OF THE NATIONAL COMMUNICATIONS FORUM vol. 42, no. 2, 30 Septembre 1988, OAK BROOK (US) pages 1706 - 1713; P E. JACKSON ET AL: 'portable communication '

TELCOM REPORT vol. 12, no. 5, 1989, M}NCHEN (DE) pages 142 - 145; H. AUSPURG: 'Intelligente Netze beschleunigen Einf}hrung neuer Dienste ';

ABSTRACT EP 459065 A1 (Translated)

In response to a call request (LID) emanating from the autonomous station (SP) and in the presence of a loading request signal, the control means (UTF) investigate all the telephone subscription data relating to the autonomous station (SP) as well as that indicating the remote-loading order. The enciphering means (CDF) encipher, with the aid of the special key (EPID), those which are secret (PIN). The processing means (UTF) allow the transmission in clear of the telephone subscription data which are public, as well as those which are secret and so enciphered, to the said autonomous station (SP) as a function of the remote-loading order.

At the level of the autonomous station (SP) the deciphering means (CDP) decipher the telephone subscription data which are secret, enciphered and so received with the aid of the special key (EPID), and the processing means (UTP) store the subscription data which are public so transmitted in clear, and secret so deciphered in the memory of the autonomous station (SP).

TRANSLATED ABSTRACT WORD COUNT: 167

ABSTRACT EP 459065 A1

En reponse a une demande d'appel (LID) emanant de la station autonome (SP) et en presence d'un signal de demande de chargement, les moyens de commande (UTF) recherchent toutes les donnees d'abonnement telephonique relatives a la station autonome (SP) ainsi que celle indiquant l'ordre de chargement a distance. Les moyens de chiffrement (CDF) chiffrent a l'aide de la cle particuliere (EPID) celles qui sont secretes (PIN). Les moyens de traitement (UTF) autorisent la transmission des donnees d'abonnement telephonique publiques en clair ainsi que celles secretes ainsi chiffrees vers ladite station autonome (SP) en fonction de l'ordre de chargement a distance.

Au niveau de la station autonome (SP) les moyens de dechiffrement (CDP) dechiffrent les donnees d'abonnement telephonique secretes chiffrees ainsi recues a l'aide de la cle particuliere (EPID), et les moyens de traitement (UTP) stockent les donnees d'abonnement publiques ainsi transmises en clair et secretes ainsi dechiffrees dans la memoire de la station autonome (SP). (voir 1 image dans le document original)

ABSTRACT WORD COUNT: 164

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	911204	A1	Published application (Alwith Search Report ;A2without Search Report)
Examination:	920226	A1	Date of filing of request for examination: 911220
Examination:	940202	A1	Date of despatch of first examination report: 931221
Change:	941228	A1	Representative (change)
*Assignee:	941228	A1	Applicant (transfer of rights) (change): FRANCE TELECOM (1334140) 6, Place d'Alleray F-75015 Paris (FR) (applicant designated states: DE;FR;GB)
Grant:	950405	B1	Granted patent
Oppn None:	960327	B1	No opposition filed

LANGUAGE (Publication,Procedural,Application): French; French; French

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	EPAB95	2290

```
      CLAIMS B   (German)  EPAB95     2015
      CLAIMS B   (French)  EPAB95     2320
      SPEC B     (French)  EPAB95     6738
Total word count - document A            0
Total word count - document B        13363
Total word count - documents A + B   13363
```

...CLAIMS their transform (S1, S2) by means of a cryptographic function F using the special key (**PIN**) and an **additional variable** datum (EPIN3) generated by the control means of the auxiliary enabling means.
15. Installation according...

...CLAIMS transforme (S1, S2) par une fonction cryptographique F a l'aide de la cle particuliere (**PIN**) et d'une donnee **variable supplementaire** (EPIN3) generee par les moyens de commande des moyens d'autorisation auxiliaires.
15. Installation selon...

37/5,K/32 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

01066458 **Image available**
SECURE WIRELESS LOCAL OR METROPOLITAN AREA NETWORK AND RELATED METHODS
RESEAU LOCAL OU METROPOLITAIN SANS FIL SECURISE ET PROCEDES S'Y RAPPORTANT
Patent Applicant/Assignee:
HARRIS CORPORATION, 1025 W. NASA Blvd., Melbourne, FL 32919, US, US (Residence), US (Nationality)
Inventor(s):
BILLHARTZ Thomas Jay, 2355 Polonius Lane, Melbourne, FL 32934, US,
FLEMING Frank Joseph, 601 Morning Cove Circle, Palm Bay, FL 32909, US,
Legal Representative:
YATSKO Michael S (agent), Harris Corporation, 1025 W. NASA Blvd., Melbourne, FL 32919, US,
Patent and Priority Information (Country, Number, Date):

```
  Patent:               WO 200396614 A1 20031120 (WO 0396614)
  Application:          WO 2003US14324 20030507  (PCT/WO US0314324)
  Priority Application: US 2002143153 20020510
```

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: **H04L-009/22**
International Patent Class: **H04L-009/00** ; G06F-017/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 4438

English Abstract
A secure wireless local or metropolitan area network (10) and data communications devices therefore are provided (11n), where the device (11n) transmits plain text in an encrypted message including cipher text

and an initialization vector. The device may include a seed generator (20) for performing a one-way algorithm using a secret key, a device address, and a changing reference value for generating a seed. Further, a random initialization vector (IV) generator (21) may be included for generating a random IV, and a key encryptor (22) may generate a key sequence based upon the seed and the random IV. Additionally, a logic circuit (23) may be included for generating cipher text based upon the key sequence and plain text, and a wireless communications device (25) may be connected to the logic circuit (23) and the random IV generator (21) for wirelessly transmitting the encrypted message.

French Abstract

L'invention concerne un reseau local ou metropolitain sans fil securise (10) et leurs dispositifs de communications de donnees (11n). Ces dispositifs (11n) transmettent des textes clairs dans un message crypte comprenant un cryptogramme et un vecteur d'initialisation. Le dispositif peut comprendre un generateur de graines (20) servant a mettre en oeuvre un algorithme unilateral au moyen d'une cle secrete; une adresse du dispositif; et une valeur de reference variable pour generer une graine. Un generateur (21) de vecteur d'initialisation aleatoire (IV) peut en outre etre inclus pour generer un vecteur d'initialisation aleatoire; et un crypteur de cles (22) peut produire une sequence cle basee sur la graine et le vecteur d'initialisation aleatoire. De plus, un circuit logique (23) peut etre inclus pour produire un cryptogramme base sur la sequence cle et le texte clair; et un dispositif de communications sans fil (25) peut etre connecte au circuit logique (23) et au generateur (21) de vecteur d'initialisation aleatoire pour transmettre sans fil le message crypte.

```
Legal Status (Type, Date, Text)
Publication  20031120 A1 With international search report.
Publication  20031120 A1 Before the expiration of the time limit for
                         amending the claims and to be republished in the
                         event of the receipt of amendments.
```

Main International Patent Class: **H04L-009/22**
International Patent Class: **H04L-009/00** ...
Fulltext Availability:
  Detailed Description
  Claims

Detailed Description

... wireless communications device may have associated therewith a media access controller (MAC) layer, and the **changing** reference **value** may be a MAC layer **sequence** **number** . By way of example, the **changing** reference **value** may have a size greater than or equal to about 12 bits.

The use of...

...is updated with each encrypted message that is sent. In accordance with the invention, the **changing** reference **value** may conveniently be the MAC layer **sequence** **number** , although other **changing** reference **values** may be generated or used for creating the key seed. By way of example, the...

...equal to about 12 bits, which is the typical size of the MAC layer **sequence** **number** . By using a 12-bit **changing** reference **value** , for example, a decryption dictionary attack would have to be 4096 times as large as...

Claim
... wireless
communications device has associated therewith a media access controller (MAC) layer; and wherein the **changing** reference **value** comprises a MAC layer **sequence** **number** .

4 The device of Claim 1 further comprising an integrity checker for generating an integrity...

37/5,K/33 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

01066457 **Image available**
SECURE MOBILE AD-HOC NETWORK AND RELATED METHODS
RESEAU AD HOC MOBILE SECURISE ET PROCEDES ASSOCIES
Patent Applicant/Assignee:
HARRIS CORPORATION, 1025 W. Nasa Blvd., Melbourne, FL 32919, US, US (Residence), US (Nationality)
Inventor(s):
BILLHARTZ Thomas Jay, 2355 Polonius Lane, Melbourne, FL 32934, US,
FLEMING Frank Joseph, 601 Morning Cove Circle, Palm Bay, FL 32909, US,
Legal Representative:
YATSKO Michael S (et al) (agent), Harris Corporation, 1025 W. Nasa Blvd, Melbourne, FL 32919, US,
Patent and Priority Information (Country, Number, Date):

Patent:	WO 200396606 A1 20031120	(WO 0396606)
Application:	WO 2003US14322 20030507	(PCT/WO US0314322)
Priority Application:	US 2002143145 20020510	

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: **H04L-009/00**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 4654

English Abstract

A mobile ad-hoc network (10) may include a plurality of nodes including a source node (11a) and at least one adjacent node (11b). The source node (11a) may include a wireless communications device for establishing a wireless communication link with the at least one adjacent node (11b), a plain text source (24), and a second generator (20) for performing a one-way algorithm using a secret key for generating a seed. Furthermore, the source node (11a) may also include a key encryptor (22) for receiving the seed and generating a key sequence based thereon, and a logic circuit for generating a cipher text for transmission over the wireless communications link and based upon the key sequence and the plain text.

French Abstract

L'invention concerne un reseau ad hoc mobile (10) pouvant comprendre une pluralite de noeuds, dont un noeud source (11a) et au moins un noeud adjacent (11b). Le noeud source (11a) peut comprendre un dispositif de communication sans fil destine a etablir une liaison de communication sans fil avec le noeud adjacent (11b), une source de texte en clair (24) et un generateur de valeur de depart (20) servant a executer un algorithme unidirectionnel utilisant une cle secrete pour generer une valeur de depart. En outre, le noeud source (11a) peut egalement comprendre un crypteur de cle (22) destine a recevoir la valeur de depart et a generer une sequence de cle sur la base de celle-ci, ainsi qu'un circuit logique permettant de generer un cryptogramme en vue d'une transmission sur la liaison de communication sans fil et sur la base de la sequence de cle et du texte en clair.

```
Legal Status (Type, Date, Text)
Publication  20031120 A1 With international search report.
Examination   20040205 Request for preliminary examination prior to end of
                       19th month from priority date
```

Main International Patent Class: **H04L-009/00**

Fulltext Availability:
  Detailed Description

Detailed Description

... wireless communications device may have associated therewith a media access controller (MAC) layer, and the **changing** reference **value** may be a MAC layer **sequence** **number** , for example. Further, the seed generator may perform the one-way algorithm using the secret...

...is updated with each encrypted message that is sent. In accordance with the invention, the **changing** reference **value** may conveniently be the MAC layer **sequence** **number** , although other **changing** reference **values** may be generated or used for creating the key seed.

By way of example, the...

...or equal to about 12 bits, which is the typical size of the MAC layer **sequence** **number** . By using a 12-bit **changing** reference **value** , for example, other types of message comparison attacks, such as a decryption dictionary attack, would...

37/5,K/42 (Item 11 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00987172 **Image available**

WEB-BASED SECURITY WITH CONTROLLED ACCESS TO DATA AND RESOURCES

SECURITE SUR LA TOILE A ACCES AUX DONNEES ET RESSOURCES SURVEILLE

Patent Applicant/Assignee:
  HUMANA INC, HUM23, 500 West Main Street, Louisville, KY 40202, US, US (Residence), US (Nationality)

Inventor(s):
  EDWARDS Brett T, 5002 Cool Brook Road, Louisville, KY 40291, US,
  LAWHEAD Aaron L, 3134 Whiteblossom Circle, Albany, IN 47150, US,
  ROSENBERG Siddy, 7102 Wood Briar Road, Louisville, KY 40241, US,
  KEINSLEY Brian E, 2925 Corydon Ridge Road NE, Corydon, IN 47112, US,

LIGHT Eric P, 511 Belgravia Court, Louisville, KY 40203, US,
TOWNSEND David L, 623 Floral Terrace, Louisville, KY 40208, US,
HARRIS Sharon A, 1320 Mount Pleasant Road, Villanova, PA 19085, US,
LATIMER Eleanor W, 5111 Pebblebrook Drive, Dallas, TX 75229-5502, US,
WEBER Leigh S, 1420 Glenn Drive, Maple Glen, PA 19002, US,
SMITHSON Mark A, 12110 Greenvalley Drive, Louisville, KY 40243, US,
STANLEY Craig, 3431 Justinian, Jeffersonville, IN 47130, US,
BURCHARD William, 9306 Talitha Drive, Louisville, KY 40299, US,
Legal Representative:
SHAPIRO Linda J (et al) (agent), Jacobson Holman, PLLC, The Jenifer Building, 400 Seventh Street, NW, Washington, DC 20004, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200317096 A1 20030227 (WO 0317096)
Application: WO 2002US25272 20020812 (PCT/WO US0225272)
Priority Application: US 2001311821 20010814
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU
CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP
KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO
RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-009/445
International Patent Class: G06F-007/00; G06F-017/60; G06F-017/00;
H04L-009/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 40811

English Abstract

A stand-alone security system controlling access to secured information and self-service functionality for a sponsor organization, usable for Web-based and IVR-based self-service functions, having five primary facets: (1) control of access to secured information (2) enabling access to users having indirect and direct relationships with the sponsor organization (3) distribution of security administration from a central information technology resource to users of the security system, (4) support for integration into different environments, and (5) support for system integrators. Key components of access control include (1) association of a userID with one specific person, (2) identification of keys to data in back-end systems and association of those keys with the system users, (3) definition of pieces (segments) of an organization so that permissions are granted based on the pieces, (4) definition of user roles based on the functionality to which he has been given permission, (5) a single sign-on for a user with multiple reasons to use the system, and (6) support for direct and indirect assignment of business functions.

French Abstract

L'invention concerne un systeme de securite autonome ayant pour mission de surveiller l'acces aux informations securisees et a la fonctionnalite libre-service dans le cadre d'une organisation de parrainage, offrant des fonctions de libre-service sur la Toile et dans un systeme RVI et presentant cinq facettes principales: (1) surveillance de l'acces aux informations securisees, (2) acces aux utilisateurs ayant un lien indirect et direct avec l'organisation de parrainage, (3) distribution de l'administration de securite a partir d'une ressource de technologie d'information centrale aux utilisateurs du systeme securise, (4) support

dans le cadre de l'integration a differents environnements, (5) support aux integrateurs de systemes. Les composants cles de la surveillance de l'acces sont constitues de (1) l'association d'une identification utilisateur avec une personne specifique, (2) l'identification de touches a des donnees dans un systeme de fond et l'association de ces touches avec les utilisateurs du systeme, (3) la definition de pieces (segments) d'une organisation de maniere que les autorisations donnees dependent des pieces, (4) la definition des roles de l'utilisateur selon la fonctionnalite a laquelle ils ont droit, (5) une seule ouverture de session pour un utilisateur ayant de multiples raisons d'utiliser le systeme, et (6) le support dans le cadre d'attributions directes et indirectes de fonctions commerciales.

Legal Status (Type, Date, Text)
Publication 20030227 A1 With international search report.
Publication 20030227 A1 With amended claims.
Examination 20030530 Request for preliminary examination prior to end of 19th month from priority date

...International Patent Class: **H04L-009/00**
Fulltext Availability:
Detailed Description

Detailed Description
... of Origin may also initiate the PIN/Password change process by posting the User ID, **PIN / Password** and a **PIN / Password change value** of I to a specified variable in the page referenced above.

6. Defining a PO...

37/5,K/43 (Item 12 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00985143 **Image available**
METHOD AND APPARATUS FOR A ROLLING CODE LEARNING TRANSMITTER
PROCEDE ET DISPOSITIF POUR EMETTEUR A APPRENTISSAGE DE CODE DE BRASSAGE
Patent Applicant/Assignee:
THE CHAMBERLAIN GROUP INC, 845 Larch Avenue, Elmhurst, IL 60126, US, US (Residence), US (Nationality)
Inventor(s):
FITZGIBBON James J, 1521 Hadley Drive, Batavia, IL 60510, US,
Legal Representative:
SAMPLES Kenneth H (et al) (agent), Fitch, Even, Tabin & Flannery, 120 South LaSalle Street, Suite 1600, Chicago, IL 60603, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200315327 A1 20030220 (WO 0315327)
Application: WO 2002US25144 20020808 (PCT/WO US0225144)
Priority Application: US 2001925867 20010809
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04K-001/00
International Patent Class: **H04L-009/00** ; G08C-019/00
Publication Language: English

Filing Language: English
Fulltext Availability:
  Detailed Description
  Claims
Fulltext Word Count: 7346

English Abstract

A barrier movement operator system having a receiver for receiving (80), learning and responding to transmitted rolling code type access codes; at least one trained transmitter (30) for operation the system by transmitting a rolling code type access code to the receiver; at least one learning transmitter (31) for learning the rolling code type access code from said trained transmitter in order to operate the system; a controller (70) for evaluating the relationship between the learning transmitter rolling type access code and the trained transmitter rolling type access code; and a device for providing a barrier movement in response to access codes received by the receiver.

French Abstract

L'invention concerne un systeme d'operateur a mouvement de barriere, dote des equipements suivants: recepteur pour la reception (80) et l'apprentissage de codes d'acces du type code de brassage, et pour la reponse a de tels codes; au moins un emetteur deja rompu a ce genre de code (30) pour l'exploitation du systeme par le biais de la transmission de code du type code de brassage au recepteur; au moins un emetteur en apprentissage (31), apprenant du premier emetteur le type de code considere pour l'exploitation du systeme; un controleur (70) evaluant la relation entre le code d'acces de type code de brassage pour emetteur en apprentissage et le code d'acces de type code de brassage pour emetteur deja rompu a ce genre de code; et un dispositif assurant un mouvement de barriere en reponse aux codes d'acces recus par le recepteur.

Legal Status (Type, Date, Text)
Publication 20030220 A1 With international search report.

International Patent Class: **H04L-009/00** ...
Fulltext Availability:
  Detailed Description

Detailed Description
... a fixed switch identification portion. The fixed 1 5 transmitter identification is a unique transmitter **identification** **number** . The rolling portion is a **number** that **changes** every transmission in
? t37/5,k/56,61,65,75-76,78,81,85-86,88,96

37/5,K/56   (Item 25 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00863834   **Image available**
SYSTEM AND METHOD FOR CONTROLLING THE ACCESS TO DIGITAL WORKS THROUGH A NETWORK
SYSTEME ET PROCEDE PERMETTANT DE CONTROLER L'ACCES A DES TRAVAUX NUMERIQUES METTANT EN OEUVRE D'UN RESEAU
Patent Applicant/Assignee:
  MEDIASHELL CORP, 90 Richmond St.E., Suite 210, Canada M5C 1P1, CA, CA (Residence), CA (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
  AUER Anthony R, 5 Vergorda Circle, St. Catharines, Ontario L2T 2P1, CA, CA (Residence), CA (Nationality), (Designated only for: US)
  SIMMONS Stanley J, 733 Downing Street, Kingston, Ontario K7M 5N1, CA, CA

(Residence), CA (Nationality), (Designated only for: US)
YEUNG Eric C H, 322 Eglinton Ave.E., Apt. 804, Toronto, Ontario, Canada M4P 1L6, CA, CA (Residence), CA (Nationality), (Designated only for: US)

Legal Representative:
WILKES Robert H (agent), 72 Albany Ave., Toronto, Ontario M5R 3C3, CA,

Patent and Priority Information (Country, Number, Date):

```
  Patent:               WO 200197480 A2-A3 20011220 (WO 0197480)
  Application:          WO 2001CA883 20010612  (PCT/WO CA0100883)
  Priority Application: US 2000210771 20000612
```

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM

Main International Patent Class: H04L-029/06
International Patent Class: G06F-001/00; **H04L-009/32** ; G06F-017/60
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 6955

English Abstract

Controlled access to digital works (104) employs a dynamically updated client identification code (214) to uniquely identify the client (100) to a server, content identification code (212) to identify digital work, and a client software module (210) as an agent of the server (102). An encrypted secret (218) unencrypted authorization code allowing access to the data content is transmitted to the client (100). Transmitting an encrypted secret (218) to the client (100) over an insecure communications network (104) supports encryption of the digital work. A database association provides for a software license environment for copies of different digital works and at least one machine. Distributing supplemental data content (e.g. advertising) from one or many servers (102) to a client (100) involves contacting an authentication server to determine whether access to the primary digital work should be provided to the client (100), retrieving from a data content server the supplemental data content and transmitting the supplemental data content to the client (100) for display.

French Abstract

L'invention concerne un acces controle a des travaux numeriques mettant en oeuvre un reseau, qui fait appel a un code d'identification client mis a jour de maniere dynamique afin d'identifier un client unique a un serveur, un code d'identification de contenu permettant d'identifier un travail numerique, et un module logiciel client utilise en tant qu'agent du serveur. Un secret crypte ou un code d'autorisation non crypte, permettant l'acces au contenu de donnees, est transmis au client. La transmission d'un secret crypte au client dans un reseau de communication non securise prend en charge le cryptage du travail numerique. Une association de bases de donnees fournit un environnement licence d'utilisation logicielle pour des copies de differents travaux numeriques et au moins une machine. La distribution de contenu de donnees additionnel (par ex. de la publicite) a partir d'un ou de plusieurs serveurs a un client implique de contacter un serveur d'authentification afin de determiner si l'acces au travail numerique primaire doit etre

fourni au client, d'extraire d'un serveur de contenu de donnees le contenu de donnees additionnel et de transmettre ce contenu de donnees additionnel au client pour affichage.

```
Legal Status (Type, Date, Text)
Publication  20011220 A2 Without international search report and to be
                         republished upon receipt of that report.
Examination    20020321 Request for preliminary examination prior to end of
                         19th month from priority date
Search Rpt     20020801 Late publication of international search report
Republication 20020801 A3 With international search report.
Search Rpt     20020801 Late publication of international search report
Correction     20021205 Corrected version of Pamphlet: pages 1/11-11/11,
                         drawings, replaced by new pages 1/11-11/11; due to
                         late transmittal by the receiving Office;
Republication 20021205 A3 With international search report.
```

...International Patent Class: **H04L-009/32**
Fulltext Availability:
  Detailed Description
  Claims

Detailed Description
... identification code as a concatenation of a fixed identifier unique to the server, a
3
changeable sequence number incremented by the server, and a **changeable** pseudo-random **number** ; and at every authorizafion contact of a client with a server, updating the client and...

Claim
... the identification code as a concatenation of a fixed identifier unique to a server, a **changeable sequence number** incremented by the server, and a **changeable**
pseudo-random **number** ; and
at every authorization contact of a client with the server, updating the client and...

37/5,K/61 (Item 30 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00830343 **Image available**
INTEGRITY CHECK IN A COMMUNICATION SYSTEM
CONTROLE D'INTEGRITE DANS UN SYSTEME DE COMMUNICATION
Patent Applicant/Assignee:
  NOKIA NETWORKS OY, Keilalahdentie 4, FIN-02150 Espoo, FI, FI (Residence), FI (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
  VIALEN Jukka, Haltiantie 3C, FIN-02300 Espoo, FI, FI (Residence), FI (Nationality), (Designated only for: US)
  NIEMI Valtteri, Topeliuksenkatu 32 G 11, FIN-00290 Helsinki, FI, FI (Residence), FI (Nationality), (Designated only for: US)
Legal Representative:
  RUUSKANEN Juha-Pekka (et al) (agent), Page White & Farrer, 54 Doughty Street, London WC1N 2LS, GB,
Patent and Priority Information (Country, Number, Date):
  Patent: WO 200163954 A1 20010830 (WO 0163954)
  Application: WO 2001EP735 20010123 (PCT/WO EP0100735)

Priority Application: GB 20004178 20000222
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ
DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ
LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG
SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04Q-007/38
International Patent Class: **H04L-009/32**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 9464

English Abstract

A method of communication between a first node and a second node for a system where a plurality of different channels is provided between said first and second node. The method comprises the step of calculating an integrity output. The integrity output is calculated from a plurality of values, some of said values being the same for said different channels. At least one of said values is arranged to comprise information relating to the identity of said channel, each channel having a different identity. After the integrity output has been calculated, information relating to the integrity output is transmitted from one of said nodes to the other.

French Abstract

L'invention concerne un procede de communication entre un premier noeud et un second noeud destine a un systeme comprenant une pluralite de canaux differents entre le premier et le second noeud. Ledit procede consiste a calculer une sortie d'integrite a partir d'une pluralite de valeurs, certaines de ces valeurs etant equivalentes pour les differents canaux. Certaines desdites valeurs au moins sont concues pour contenir des informations relatives a l'identite dudit canal, chaque canal ayant une identite differente. Apres le calcul de la sortie d'integrite, les informations relatives a la sortie d'integrite sont transmises d'un des noeuds precites a l'autre.

Legal Status (Type, Date, Text)
Publication 20010830 A1 With international search report.

International Patent Class: **H04L-009/32**
Fulltext Availability:
Detailed Description

Detailed Description
... in addition to the secret integrity key and the message.

In the case where a **sequence** of **numbers** are used as time **varying parameters** , a mechanism is used which prevents the

37/5,K/65 (Item 34 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00802024 **Image available**

METHOD AND APPARATUS FOR PRESENTING ANONYMOUS GROUP NAMES
PROCEDE ET APPAREIL DE PRESENTATION DE NOMS DE GROUPES ANONYMES

Patent Applicant/Assignee:
SUN MICROSYSTEMS INC, 901 San Antonio Road, MS UPALI-521, Palo Alto, CA 94303, US, US (Residence), US (Nationality)

Inventor(s):
HANNA Stephen R, 3 Beverly Road, Bedford, MA 01730, US,
ANDERSON Anne H, 28 Minuteman Road, Acton, MA 01720, US,
ELLEY Yassir K, 664-B South Street, Waltham, MA 02453, US,
PERLMAN Radia J, 10 Huckleberry Lane, Acton, MA 01720, US,
MULLAN Sean J, 29 Merrion Strand, Sandymount Dublin-4, IE,

Legal Representative:
LEBOVICI Victor B (et al) (agent), Weingarten, Schurgin, Gagnebin & Hayes, LLP, Ten Post Office Square, Boston, MA 02109, US,

Patent and Priority Information (Country, Number, Date):

Patent:	WO 200135574 A1 20010517 (WO 0135574)
Application:	WO 2000US41197 20001017 (PCT/WO US0041197)
Priority Application:	US 99439246 19991112

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM

Main International Patent Class: **H04L-009/32**
International Patent Class: **H04L-009/00**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 8632

English Abstract

A method and system for granting an applicant associated with a client computer (10) in a client-server system access to a requested service without providing the applicant with intelligible information regarding group membership. The applicant transmits a request for service to an application server (12) over a computer network (14). In response, the server determines which group or groups are authorized to obtain access to the service. The application server then prepares an encrypted message which includes the identification of the group or groups having access privileges and transmits the encrypted message to the client along with a request that the client prove membership in at least one of the groups. The client forwards the encrypted message to the group membership server (16a) which decrypts the message and prepares a certificate or other proof of membership.

French Abstract

L'invention se rapporte a un procede et a un systeme permettant d'accorder, a un demandeur associe a un ordinateur client (10) d'un systeme client-serveur, l'acces a un service demande sans delivrer au demandeur des informations intelligibles concernant l'appartenance a un groupe. Le demandeur emet une demande de service a un serveur d'applications (12) sur un reseau informatique (14). En reponse, le serveur determine quel est ou quels sont les groupes autorise(s) pouvant acceder au service. Le serveur d'applications prepare ensuite un message chiffre qui contient l'identification du groupe ou des groupes ayant des privileges d'acces et emet le message chiffre a destination du client

ainsi qu'une demande adressee au client pour que celui-ci prouve son appartenance a au moins l'un des groupes. Le client transmet le message chiffre au serveur qui gere l'appartenance aux groupes (16a) et qui dechiffre le message et prepare un certificat ou une autre preuve d'appartenance au groupe.

Legal Status (Type, Date, Text)
Publication 20010517 A1 With international search report.

Main International Patent Class: **H04L-009/32**
International Patent Class: **H04L-009/00**
Fulltext Availability:
Detailed Description

Detailed Description
... group identifier, may comprise a random number, a pseudo-random number, a number within a **sequence** of **numbers** , a date and time value, or any other **value** which **changes** each time the message generated by the group membership server is generated.

While the above...

...64. The extension may be a random number, pseudo-random number, a number within a **sequence** of **numbers** , a date and time or any other **value** , which **changes** each time the value is generated. The extended group identifier is then encrypted as illustrated

37/5,K/75 (Item 44 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00748792 **Image available**
CREDIT CARD SECURITY TECHNIQUE
TECHNIQUE DE SECURITE POUR CARTE DE CREDIT
Patent Applicant/Assignee:
CLEARTOGO COM, Amnon Ve-Tamar Street 12, 46417 Herzliya, IL, IL (Residence), IL (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
SOLBERG Yoram, Amnon Ve-Tamar Street 12, 46417 Herzliya, IL, IL (Residence), IL (Nationality), (Designated only for: US)
BERLIN Arie, Yoram Solberg, Amnon Ve-Tamar Street 12, 46417 Herzliya, IL, IL (Residence), IL (Nationality), (Designated only for: US)
Legal Representative:
SANFORD T COLB & CO, P.O. Box 2273, 76122 Rehovot, IL
Patent and Priority Information (Country, Number, Date):
Patent: WO 200062214 A1 20001019 (WO 0062214)
Application: WO 2000IL211 20000406 (PCT/WO IL0000211)
Priority Application: IL 129361 19990408; US 2000174476 20000103
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-017/60

International Patent Class: H04K-001/00; **H04L-009/00**
Publication Language: English
Filing Language: English
Fulltext Availability:
  Detailed Description
  Claims
Fulltext Word Count: 12820

English Abstract

A technique for secure electronic commerce is disclosed wherein a transaction initiator (26) has a primary identifier and a list of secondary identifiers stored therein, each of which is valid for a single transaction. An identification center (36) receives the primary and secondary verification numbers and verifies that the primary number is valid and that the secondary number is appropriate for a current transaction using the primary number. The transaction initiator comprises an enhanced monetary card, such as a credit card or a stored value card, which includes an embedded processor, and which provides the secondary number for each transaction. The secondary numbers are stored in a lookup table, which is also available to the identification center. The values in the lookup table are indexed according to a transaction counter and are preferably communicated to the identification center without encryption or challenge. In some embodiments the transaction initiator comprises other types of hardware such as a personal computer in conjunction with secondary memory such as a CDr for storing secondary numbers and software.

French Abstract

L'invention concerne une technique de commerce electronique securisee dans laquelle un initiateur de transaction (26) comprend un identificateur primaire ainsi qu'une liste d'identificateurs secondaires memorises dans celui-ci, dont chacun est valide pour une seule transaction. Un centre d'identification (36) recoit les numeros de verification primaire et secondaire et verifie que le numero primaire est valide et que le numero secondaire convient a une transaction en cours a l'aide du numero primaire. L'initiateur de transaction comprend une carte monetaire evoluee telle qu'une carte de credit ou une carte a valeur memorisee, laquelle contient un processeur integre, et laquelle fournit le numero secondaire pour chaque transaction. Les numeros secondaires sont memorises dans une table de consultation, laquelle est egalement disponible pour le centre d'identification. Les valeurs dans la table de consultation sont indexees selon un compte de transaction et sont de preference transmises au centre d'identification sans chiffrement ou intervention. Dans certains modes de realisation, l'initiateur de transaction comprend d'autres types de materiel tels qu'un ordinateur personnel en association avec une memoire secondaire tel qu'un CDr destine a memoriser des numeros secondaires et du logiciel.

```
Legal Status (Type, Date, Text)
Publication    20001019 A1 With international search report.
Publication    20001019 A1 Before the expiration of the time limit for
                           amending the claims and to be republished in the
                           event of the receipt of amendments.
Examination    20010222 Request for preliminary examination prior to end of
                           19th month from priority date
```

...International Patent Class: **H04L-009/00**
Fulltext Availability:
  Detailed Description

Detailed Description

... device, referred to herein as a transaction initiator, which is identified by a fixed: primary **identification number** and a **varying** secondary **identification number** . An identification center (or centers) receives the primary and secondary verification numbers and verifies that...and prevents unauthorized use of the card in case it is lost, and the secondary **number** which **changes** with each transaction. It is noted that the term " **identification number** " is used herein in a general way to refer to any type of code.

It...

37/5,K/76 (Item 45 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00736251 **Image available**
COMMAND CONSOLE FOR HOME MONITORING SYSTEM
CONSOLE DE COMMANDE POUR SYSTEME DOMOTIQUE
Patent Applicant/Assignee:
EARLY WARNING CORPORATION, P.O. Box 4476, Wheaton, IL 60189-4476, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
QUIGLEY Mark P, 3S440 Herrick Road, Warrenville, IL 60555, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
PENN Amir N, McDonnell Boehnen Hulbert & Berghoff, 32nd floor, 300 South Wacker Drive, Chicago, IL 60606, US
Patent and Priority Information (Country, Number, Date):
Patent: WO 200049589 A1 20000824 (WO 0049589)
Application: WO 2000US4568 20000222 (PCT/WO US0004568)
Priority Application: US 99255421 19990222
Designated States: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G08B-019/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 91331

English Abstract
A method and apparatus for a home monitoring system is provided. The home monitoring system may include a command console (10) for monitoring and processing the output of sensors (14, 16, 18, 20, 22, 24). The processing of the sensors (14, 16, 18, 20, 22, 24) includes (1) providing a history of the sensor as an indicator to the operator of the sensor output over time; (2) analyzing the trends of the sensor to increase the effectiveness of the sensor beyond simply the current sensor output; and (3) analyzing the output of one sensor which may impact interpretation of a second sensor's output. The monitoring system may also be a prescription reminder system. The prescription reminder system may be used in homes or institutional medical facilities (assisted living or nursing homes) to provide patients with a manner to remind them to take

pharmaceutical drugs at prescribed times.

French Abstract

Il s'agit d'un procede et d'un dispositif utilises pour un systeme domotique. Ce systeme domotique peut comprendre une console de commande (10) pour controler et traiter les sorties de capteurs (14, 16, 18 20, 22, 24). Le traitement des capteurs (14, 16, 18, 20, 22, 24) vise a (1) fournir un historique du capteur qui servira d'indicateur a l'operateur sur les sorties du capteur au fil du temps; (2) analyser les tendances du capteur pour ameliorer son efficacite au-dela des seules sorties du capteur courant; et (3) analyser les sorties d'un capteur susceptibles d'avoir une incidence sur l'interpretation des sorties d'un deuxieme capteur. Le systeme de surveillance peut egalement servir d'aide-memoire pharmaceutique. Cet aide-memoire pharmaceutique peut etre utilise dans des centres ou des etablissements de soins (maisons de retraite ou maisons de repos) et servir aux patients pour les avertir aux heures prescrites de prise des medicaments

```
Legal Status (Type, Date, Text)
Publication    20000824 A1 With international search report.
Examination    20010412 Request for preliminary examination prior to end of
                        19th month from priority date
```

Fulltext Availability:
  Claims

Claim

... the menus
appropriately
void godmenu (void
* We're going to 1 of 6 places:
* (1) **Add / Change** Parent **PIN Number** (GOD Mode)
* (2) **Add / Change** Child **PIN Number** (PEON Mode)
* (3) **Add / Change** General **PIN Number** (PEON Mode)
* (4) Configure System
* (5) Activate/Deactivate Burglar Alarm (if Burglar sensors exist)
* (6...

37/5,K/78 (Item 47 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

(c) 2004 WIPO/Univentio. All rts. reserv.

00532353 **Image available**

METHOD AND APPARATUS FOR SECURING SOFTWARE TO REDUCE UNAUTHORIZED USE

PROCEDE ET DISPOSITIF DE SECURISATION D'UN LOGICIEL, DESTINES A REDUIRE UN USAGE NON AUTORISE DE CELUI-CI

Patent Applicant/Assignee:
  COLVIN David S,

Inventor(s):
  COLVIN David S,

```
Patent and Priority Information (Country, Number, Date):
  Patent:               WO 9963705 A1 19991209
  Application:          WO 99US11647 19990527  (PCT/WO US9911647)
  Priority Application: US 9890620 19980604
```

Designated States: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE
ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT
LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT
UA UG US UZ VN YU ZA ZW GH GM KE LS MW SD SL SZ UG ZW AM AZ BY KG KZ MD
RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF
CG CI CM GA GN GW ML MR NE SN TD TG

Main International Patent Class: **H04L-009/00**
International Patent Class: **H04L-009/06**
Publication Language: English
Fulltext Availability:
  Detailed Description
  Claims
Fulltext Word Count: 6075

English Abstract

A method and apparatus for securing software to reduce unauthorized use include associating a password (16) or series of passwords (18) with each copy or group of authorized software and requiring entry of a first password obtained from the developer or authorized representative (24) of the software after exchanging registration information (38). The method and apparatus may also require entry of a second password from the series associated with the software to continue using the software. A password (16) or authorization code series may be associated with each authorized copy or with a group of copies such as those distributed to a particular organization or site (32). Preferably, subsequent passwords (16) or authorization codes are obtained from an authorized software developer (24), manufacturer, or distributor which gathers current information from the user (30) to monitor compliance with licensing restrictions. The number and frequency of required password updates may be regular or irregular. A code which disables the software may be communicated if the manufacturer determines that the user (30) is an unauthorized user.

French Abstract

L'invention concerne un procede et un dispositif de securisation d'un logiciel, destines a reduire un usage non autorise du logiciel, le procede consistant a associer un mot de passe (16) ou une serie de mots de passe (18) a chaque copie ou groupe de logiciels autorises, et a exiger l'entree d'un premier mot de passe obtenu a partir du developpeur du logiciel ou du representant autorise (24) de celui-ci, apres echange d'informations d'enregistrement (38). Ce procede et ce dispositif peuvent egalement exiger l'entree d'un second mot de passe a partir de la serie associee au logiciel pour la continuation de l'utilisation du logiciel. Un mot de passe (16) ou une serie de codes d'autorisation peut etre associe a chaque copie autorisee ou a un groupe de copies, tel ceux distribues a une organisation ou a un site (32) en particulier. De preference, des mots de passe (16) ou codes d'autorisation ulterieurs sont obtenus a partir d'un developpeur (24), fabricant ou distributeur de logiciels autorise, lequel recueille des informations actuelles a partir de l'utilisateur (30) afin de pouvoir surveiller si cet utilisateur observe les restrictions de l'octroi de licence. Le nombre et la frequence des mises a jour des mots de passe exiges peuvent etre reguliers ou non. Un code mettant hors service le logiciel peut etre communique si le fabricant determine que l'utilisateur (30) est un utilisateur non autorise.

Main International Patent Class: **H04L-009/00**
International Patent Class: **H04L-009/06**
Fulltext Availability:
  Detailed Description

Detailed Description

... block 80. A
series of passwords may be associated with the software using an appropriate **password** generation algorithm with **parameters** which **vary** based on the particular copy. For
- 13
example, a algorithm 'or mathematical equation or formula...

37/5,K/81 (Item 50 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00510341 **Image available**
WIRELESS ROLLING CODE SECURITY SYSTEM
SYSTEME DE SECURITE SANS FIL A CODE DE BRASSAGE

Patent Applicant/Assignee:
TSUI Philip,
Inventor(s):
TSUI Philip,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9941693 A1 19990819
Application: WO 99US2902 19990210 (PCT/WO US9902902)
Priority Application: US 9823393 19980213; US 98223593 19981230
Designated States: AL AM AT AT AU AZ BA BB BG BR BY CA CH CN CU CZ CZ DE DE DK DK EE EE ES FI FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SK SL TJ TM TR TT UA UG US UZ VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Main International Patent Class: G06F-019/00
International Patent Class: G08C-019/00; G08C-019/12; H04B-009/00; E05F-015/20
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 8527

English Abstract

A processor-based transmitter-receiver system and method (10) in which a receiver (150) receives coded signals from at least two transmitters (figure 1A). The receiver (150) comprises a circuit for receiving a first coded signal from a first transmitter (140) and a second coded signal from a second transmitter (figure 3A). Each of the coded signals includes a unique identification code and a variable security code (figure 4C). A memory (102, figure 2A) stores at least two codes, each including a unique identification code and a variable security code. A processor (100, figure 2A) coupled to the circuit and the memory (102), compares each of the received coded signals with each of the stored sets of codes. The processor generates a valid signal if one of the received coded signals matches one of the stored codes.

French Abstract

L'invention concerne un systeme et un procede (10) d'emission-reception commande par processeur dans lequel un recepteur (150) recoit des signaux codes d'au moins deux emetteurs (Fig. 1A). Le recepteur (150) comprend un circuit destine a recevoir un premier signal code d'un premier emetteur (140) et un second signal code d'un second emetteur (Fig. 3A). Chacun des signaux codes comprend un code d'identification unique et un code de securite variable (Fig. 4C). Une memoire (102, Fig. 2A) enregistre au moins deux codes, chacun des codes comprenant un code d'identification unique et un code de securite variable. Un processeur (100, Fig. 2A), couple au circuit et a la memoire (102), compare chacun des signaux codes recus avec chacun des ensembles de codes enregistres. Le processeur produit un signal valide si l'un des signaux codes recus correspond a l'un des codes enregistres.

Fulltext Availability:
  Claims

Claim
... variable code;
  a memory that stores a second code, said second code including a second **identification code** and a **second variable** code;
  a second circuit coupled to said first circuit and said memory, said second circuit...first variable code;
  comparing said first code with a stored second code, including a second **identification code** and a **second variable** code; and
  initiating said alarm indication by said remote device if said first code matches...

37/5,K/85 (Item 54 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00460189 **Image available**
IMPROVED MICROCHIPS AND REMOTE CONTROL DEVICES COMPRISING SAME
MICROPUCES AMELIOREES ET DISPOSITIFS DE TELECOMMANDE LES INCLUANT
Patent Applicant/Assignee:
  MICROCHIP TECHNOLOGY INCORPORATED,
Inventor(s):
  BRUWER Frederick J,
Patent and Priority Information (Country, Number, Date):

Patent:	WO 9850653 A1 19981112	
Application:	WO 98US8817 19980504	(PCT/WO US9808817)
Priority Application:	US 97853328 19970508	

Designated States: JP KR AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: E05B-049/00
Publication Language: English
Fulltext Availability:
  Detailed Description
  Claims
Fulltext Word Count: 8149

English Abstract
  Encoder and decoder microchips suitable for use in remote control devices, are disclosed. The encoder microchip comprises means for performing an encoding function (7) on an identification number (16) embedded in the said microchip and a combination of a unit number and a stepping counter value, so as to generate a transmission value which is only decodable by a related decoding function having access to the same identification number. The decoder microchip comprises means for decoding the transmission value into a decoded unit number and a decoded counter value and means for comparing the decoded counter value with a decoder counter value range (17-20). The encoder and decoder microchips are provided with means for changing, e.g., in a preferred mode incrementing, the counter values by a number greater than one after a period of time, subsequent to the encoder microchip being activated or the decoder microchip receiving a transmission value. The encoder and decoder microchips are also provided with means for synchronizing the decoder microchip with a particular encoder microchip which has generated a synchronization command.

French Abstract
  L'invention porte sur des micropuces de codage et de decodage pour dispositifs de telecommande. La micropuce de codage comporte des moyens

permettant d'effectuer une fonction (7) de codage sur un numero d'identification inscrit dans ladite micropuce et une combinaison d'un numero (16) unitaire et d'une valeur de compteur pas-a-pas de maniere a produire une valeur de transition ne pouvant etre decodee que par une fonction de codage associee ayant acces au meme numero. La micropuce de decodage comporte des moyens de decodage des valeurs de transmission en un nombre unitaire et une valeur de compteur, et des moyens de comparaison de la valeur de compteur decodee avec la plage (17-20) de valeurs de compteur du decodeur. Les micropuces de codage et de decodage sont pourvues de moyens permettant de faire varier par exemple dans le mode prefere par incrementation les valeurs de compteur d'un nombre superieur a l'unite apres un laps de temps suite a l'activation de la micropuce de codage ou a la reception par la micropuce de decodage d'une valeur de transmission. Les micropuces de codage et de decodage sont egalement pourvues de moyens de synchronisation de la micropuce de decodage avec une micropuce particuliere de codage ayant produit une instruction de synchronisation.

Fulltext Availability:
Claims

Claim
I A system which includes an **encoder** microchip and a decoder microchip, wherein:
said **encoder** microchip comprises:
means for storing an **identification number** ,
means for storing a counter **value** ,
means for **changing** the **value** of said counter value each time the **encoder**
microchip is operated,
encoding rneans for performing a nonlinear **encoding** function on said counter value using said identification number, so as to generate a transmission...

...scan on signals so as to identify signals conforming to a specific format.

2 An **encoder** microchip comprising:
means for storing an **identification number** ;
1 5 means for storing a counter **value** ;
means for **changing** the **value** of said counter value only when the **encoder**
microchip is operated;
encoding means for perfort-ning an **encoding** function on at least said counter value using said identification number, so as to generate...

37/5,K/86 (Item 55 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00456794
BILATERAL AUTHENTICATION AND ENCRYPTION SYSTEM
SYSTEME ET PROCEDE BILATERAUX D'AUTHENTIFICATION ET DE CHIFFRAGE
Patent Applicant/Assignee:
FIELDER Guy L,
ALITO Paul N,
Inventor(s):
FIELDER Guy L,
ALITO Paul N,

Patent and Priority Information (Country, Number, Date):
Patent: WO 9847258 A2 19981022
Application: WO 98US4408 19980309 (PCT/WO US9804408)
Priority Application: US 97813457 19970310
Designated States: CA JP AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: **H04L-009/32**
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 8129

English Abstract

A bilateral system for authenticating remote transceiving stations through use of station identifiers (IDs), and through use of passwords which are used only one time, and thereafter exchanging messages through use of an encrytion key which is changed after each system connection. Upon authentication, each of the stations independently creates a secret session encryption key (27) in response to the other station's unique station identifier that is exchanged over a communication link in cleartext. The station identifiers are used as tags to look up a unique static secret (20) and a unique dynamic secret (21) which are known only by the two stations, but which are not exchanged over the communication link. The secrets are independently combined by a bit-shuffle algorithm (22), the result of which is applied to a secure hash function (23) to produce a message digest (24).

French Abstract

L'invention concerne un systeme bilateral d'authentification de stations emettrices situees a distance, au moyen d'identificateurs de station (ID), ainsi que de mots de passe utilises seulement une fois, et d'echange ensuite de messages au moyen d'une cle de chiffrage modifiee apres chaque connexion au systeme. Lors de l'authentification, chaque station cree de maniere independante une cle secrete de chiffrage de session en reponse au seul identificateur de station de l'autre station, lequel identificateur est echange en texte en clair sur une liaison de communication. Les identificateurs de station sont utilises en tant qu'etiquettes servant a rechercher un secret statique unique et un secret dynamique unique, lesquels sont connus seulement des deux stations mais ne sont pas echanges sur la liaison de communication. Ces secrets sont combines de maniere independante a l'aide d'un algorithme de melange de binaires dont le resultat est applique a une fonction de condensation sure, afin de produire un condense de message duquel sont derives la cle secrete de chiffrage de session, un mot de passe ne servant qu'une fois et destine a la station d'origine, un mot de passe ne servant qu'une fois et destine a la station receptrice, ainsi qu'une valeur de changement pseudo-aleatoire destinee a la mise a jour du secret dynamique. Ce secret dynamique est mis a jour, apres chaque connexion au systeme, au moyen de la valeur de changement pseudo-aleatoire et d'une constante primaire, provoquant ainsi la mise a jour du condense de message lors de la survenue d'une nouvelle connexion au systeme. En outre, les identificateurs de station du systeme peuvent etre modifies par une composante du condense de message lors de la survenue d'une nouvelle connexion au systeme, afin de constituer une protection supplementaire contre toute usurpation d'identite par reproduction d'informations.

Main International Patent Class: **H04L-009/32**
Fulltext Availability:
Detailed Description
Claims

Detailed Description

... Tile present invention provides a combination of authentication and encryption in which parameters including system **passwords** , encryption keys, and **change values** that are used to alter a dynamic secret to produce new, pseudo-random system passwords...

...be exchanged over a network in cleartext, and protects the encryption key generator, the system **passwords** , the encryption key, and the **change value** from public exposure. In addition, system IDs may be altered upon tile completion of a...to provide message digest 24, from which an originating system password 25, an answering system **password** 26, a secret session encryption key 27, and a **change value** 28 are extracted.

From logic step I I 1, the logic flow process continues to...

...1 12, where the answer system ID, the originating system password 25, the answering system **password** 26, the secret session encryption key 27, and the **change value** 28 are written to RAM I d of the COMPLIter system IO. The logic flow...bit-mapping to produce a message digest. The originating system password 25, the answering system **password** 26, the secret session encryption key 27 and the **change value** 28 then are extracted from the message digest at logic step 21 1 and written...

...5 area of RAM 13c.

The originating and answering systems have thus generated the same **passwords** , secret session encryption key, and **change value** without exchanging more than an access request and their respective system identifiers in cleartext.

From...

Claim

... a pseudo-random message digest comprised of an originating system password, a first answering system **password** , a session **encryption** key, and a **change value** by applying said first many-to-few bit mapping program and said second many-tofew...

...said answering system ID, for altering said one of said n dynamic secrets with said **change value** upon verification of authenticity of said second answering system **password** , for decrypting an **encrypted** answering system password with said session **encryption** key to provide said second answering system password, **encrypting** said originating system password to generate an encrypted originating system password, and upon receipt of...

...and said means for generating said pseudo-random message digest comprised of said originating system **password** , said answering system **password** , said session **encryption** key, and said **change value** , and upon verifying authenticity of said originating system ID transferring said answering system ID over...said originating system and said answering system extracting an originatingo systern password, an answering system **password** , a deterministic and symmetric **encryption** key,
and a **change value** from said message digest;
said originating system and said answering system respectively **encrypting** said
C5
originating system password and said answering system password with said deterministic and syrnmetric...set forth in Claim I I above, wherein said answering system password, said originating system **password** , said

deterministic and symmetric **encryption** key, and said **change value** are pseudo-random.

13 The method set forth in Claim I I above, wherein said...

...originating system and said answering system independently extracting an originating system password, an answering system **password** , a secret session **encryption** key,
and a **change value** from said second pseudo-random result;
said originating system transmitting said originating system password over...originating system and said answering system independently extracting an originating system password, an answering system **password** , a secret session **encryption** key,
1 5 and a **change value** from said second pseudo-random result;
encrypting said answering system **password** with said secret session **encryption** key by
said answering system to generate a first **encrypted** password;
transmitting said first **encrypted** password from said answering system to said
originating system;
decrypting and verifying said first encrypted...

37/5,K/88 (Item 57 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00455511
BILATERAL AUTHENTICATION AND INFORMATION ENCRYPTION TOKEN SYSTEM AND METHOD
SYSTEME BILATERAL A JETON D'AUTHENTIFICATION ET DE CRYPTAGE D'INFORMATIONS ET PROCEDE ASSOCIE
Patent Applicant/Assignee:
FIELDER Guy L,
ALITO Paul N,
Inventor(s):
FIELDER Guy L,
ALITO Paul N,
Patent and Priority Information (Country, Number, Date):

Patent:	WO 9845975 A2 19981015	
Application:	WO 98US4620 19980309	(PCT/WO US9804620)
Priority Application:	US 97815403 19970310	

Designated States: CA JP AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: **H04L-009/00**
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 15719

English Abstract
A first computer system (10) communicates with a second computer system (11) by way of a communication link (12). The first computer system (10) includes a central processing unit (1) with I/O interfaces (1b) leading to a keyboard processor (2) with a key matrix interface array (3). System ID's, a static secret, and a dynamic secret are stored on the hard disk drive (5b) of the first computer system (10) and are moved to RAM (1d) by the processor (1a) when the originating and answering stations are being authenticated.

French Abstract

L'invention concerne un systeme d'authentification et de cryptage de l'information, du type a jeton, pour ameliorer la securite des echanges bilateraux chiffres entre un systeme source et un systeme qui repond. Sans synchronisation, chaque systeme fournit independamment un condense de presentation des messages via un generateur de cle de cryptage, lequel utilise les techniques suivantes: brassage binaire, correspondances binaires multivoques entre beaucoup-et-peu de bits, et hachage fiable pour annihiler toute tentative de dechiffrage des entrees d'informations secretes dans le generateur, de decouverte du mot de passe du systeme, de la cle de cryptage ou bien des valeurs de changement en sortie extraites des condenses de message, suite a une analyse cryptographique ou a une serie d'attaques en force par approximations successives. Chaque systeme utilise les mots de passe, cles de cryptage et valeurs de changement durant une seule connexion systeme avant de recourir a la valeur de changement pour actualiser l'un de ces parametres, sans relation previsible avec les elements correspondants anterieurs. Chaque systeme a plusieurs cycles d'authentification permettant de verifier le systeme qui emet, le systeme qui repond, le systeme a jeton, la correspondance entre systeme a jeton et systeme qui emet ou systeme qui repond ou les deux a la fois, toujours sans devoiler ni les entrees d'informations secretes, ni les cles de cryptage ni les valeurs de changement. Il existe en outre une cle de cryptage deterministe, non previsible, pseudo-aleatoire et symetrique, utilisee durant une seule connexion systeme et detruite apres coup, ce qui dispense d'utiliser des repertoires de cles. Enfin, les identifications du systeme a jeton, du systeme qui emet et du systeme qui repond sont modifiables via un element du condense de message, lors de l'etablissement d'une connexion systeme, de maniere a reduire considerablement les risques d'usurpation d'identite sur reexecution.

Main International Patent Class: **H04L-009/00**
Fulltext Availability:
  Detailed Description
  Claims

Detailed Description
... The present invention provides a combination of authentication and encryption in which parameters including system **passwords** , encryption keys, and **change values** which are used to produce new, pseudo-random system **passwords** and encryption keys, are used during only a single system connection before being replaced with...cleartext, and protects the static and dynamic secret encryption key generator inputs, and the system **password** , encryption key, and **change value** outputs from exposure. A tamper-resistant security module or token system is used with either...

...5 other. The systems independently use such secrets to generate message digests from which systcrn **passwords** , a secret session encryption key, and a **change value** are extracted, and information encrypted with the secret session encryption key is exchanged between the systems without need for the secret session encryption key or the **change value** to be exposed in any form, or for the system **passwords** to be exposed in other than encrypted form.

In another aspect of the invention, an...
...produce a pseudo-random message digest from which an originating system password, an answering system **password** , a secret session encryption key, and a **change value** are extracted without exposure.

In a further aspect of the ...occur after each system connection to ensure that any originating system password, any answering system

password , any secret session encryption key, and any **change** **value** will be used by the originating system and the answering system during only a single...to provide message digest 24, from which an originating system password 25, an answering system **password** 26, a secret session encryption key 27, and a **change** **value** 28 are extracted.

From logic step I I 1, the logic flow process continues to...

...1 12, where the answering system ID, the originating system password 25, the answering system **password** 26, the secret session encryption key 27, and the **change** **value** 28 are WTitten to RAM I d of the com puter system IO. The logic...bit mapping to produce a message digest. The originating system password 25, the answering system **password** 26, the secret session encryption key 27 and the **change** **value** 28 then are extracted from the message digest at logic step 21 1 and written...
...an area of RAM 13c.

The originating and answering systems have thus generated the same **passwords** , secret session encryption key, and **change** **value** without exchanging more than an access request and their respective system identifiers in cleartext.

From...system, they are not exposed outside of the originating and answering systems. In addition, the **passwords** , **change** **value** , and secret session encryption key are used only during a current system connection. The dynamic...secrets and encryption key generator necessary for generating the originating system password 25, answering system **password** 26, secret session encryption key 27, and **change** **value** 28.

Referring to the functional block diagram of Figure 6, a token system 300 is...to the result to generate a message digest. At logic step 409, an originating system **password** 25, an answering system **password** 26, and a **change** **value** 28 are extracted frorn the message digest and written into operating RAM 312b. The step...flow process continues to logic step 560 where the originating system password 25, answering system **password** 26, secret session encryption key 27, and **change** **value** 28 are extracted from the message digest, and written along with the token ID into...but the secrets are never revealed by one system to the other. In addition, the **passwords** , **change** **value** , and secret session encryption key are used during only a single system connection.

The dynamic...authentication. Once a system connection is completed.

all components of an authentication exchange (originating system **password** , answering system **password** , session encryption key, and **change** **value**) are **changed** to new non-recurring values having no known relationship to the previous values. Thus, an...

Claim
... a pseudo-random message digest comprised of an originating system password, a first answering system **password** , a session **encryption** key, and a **change** **value** by applying said first many-to-few bit mapping program and said second niany-to digest comprised of said originating system **password** , said answering system **password** , said session **encryption** key, and said **change** **value** , for decrypting said **encrypted** token ID with said one of said n current **encryption** keys upon receipt from said originating system over said communication link means, and upon verifying...pseudo random result; said token system and said answering system independently extracting an originating system **password** , an answering system **password** , an **encryption** key, and a

change **value** from
said second pseudo-random result;
bilaterally authenticating said originating system and said answering system by said originating system **encrypting** said originating system password with said encryption key to produce a first encrypted password, said...token system and said answering system independently extracting an originating system password, an answering system **password** , a deterministic and symmetric **encryption** key,
·I 5 and a **change** **value** from said second pseudo-random result;
encrypting said answering system **password** with said deterministic and symmetric **encryption** key by said answerin system to generate a first **encrypted** password;
9
transmitting said first **encrypted** password from said answering system to said
originating system;
decrypting said first encrypted password by...

37/5,K/96 (Item 65 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00307239 **Image available**
METHOD AND APPARATUS FOR UTILIZING A TOKEN FOR RESOURCE ACCESS
PROCEDE ET APPAREIL D'UTILISATION D'UN JETON D'ACCES A DES RESSOURCES
Patent Applicant/Assignee:
SECURITY DYNAMICS TECHNOLOGIES INC,
Inventor(s):
WEISS Kenneth P,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9525391 A1 19950921
Application: WO 95US3181 19950316 (PCT/WO US9503181)
Priority Application: US 94213951 19940316
Designated States: AU CA JP KR AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: **H04L-009/00**
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 6295

English Abstract
The system (10) has a token (12), a token processor (14), and a host processor (16). The token (12) may be a "dumb" token, and contains a memory (18) that contains a secret user code (22) and a read/write element (20). The memory (18) may also contain a public code (24), an algorithm (26), and a time-varying value (28). The token may have a numeric keypad (30) for an imput device.

French Abstract
Ce systeme (10) possede un jeton (12), un processeur (14) de jeton et un processeur central (16). Le jeton (12) peut etre un jeton "non intelligent" et contient une memoire (18) contenant elle-meme un code utilisateur secret (22) et un element de lecture/ecriture (20). La memoire (18) peut egalement contenir un code public (24), un algorithme (26) et une valeur (28) variable en temps. Le jeton peut comporter un bloc de touches numeriques (30) pour un dispositif d'entree.

Main International Patent Class: **H04L-009/00**
Fulltext Availability:
Detailed Description
Claims

Detailed Description
... input which
is utilized along with the secret code read from token 12,
the time- **varying value** and the **PIN** in an algorithm to
generate an appropriate one-time nonpredictable coded
response (step 78). This...

Claim
... algorithm at
the token processor;
C) the token processor receiving a user inputted secret
personal **identification code** ;
d) the token processor utilizing the secret user code,
time- **varying value** and secret personal **identification code** in
the algorithm to obtain a one-time nonpredictable code;
e) the token processor transmitting...algorithm at
the token processor;
c) the token processor receiving a user inputted secret
personal **identification code** ;
d) the token processor utilizing the secret user code,
time- **varying value** and secret personal **identification code** in
the algorithm to obtain a one-time nonpredictable code;
e) the token processor transmitting...
?

```
File 347:JAPIO Nov 1976-2003/Nov(Updated 040308)
         (c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200419
         (c) 2004  Thomson Derwent

Set     Items   Description
S1     402961   PIN OR PINS OR PID OR PIDS OR UIN OR UINS
S2       6783   (SEQUENCE? ? OR SERIES)(1N)(NUMERIC? OR NUMBER? ? OR NUMER-
             AL? ? OR ALPHANUMERIC?)
S3      14274   PASSWORD? OR PASSCODE? OR PASSKEY? OR PASSNUMBER? OR PASSV-
             ALUE?
S4       1392   PASS()(WORD? ? OR KEY? ? OR CODE? ? OR NUMBER? ? OR VALUE?
              ? OR IDENTIFIER? OR ID OR SEQUENCE?)
S5      33689   (ID OR IDENTIFY? OR IDENTIFICATION? OR IDENTIFIE? ? OR AUT-
             HENTICAT? OR ACCESS OR AUTHORIZ? OR AUTHORIS?)()(CODE? ? OR N-
             UMBER? ? OR SEQUENCE)
S6          3   COENCYPHER? OR COENCIPHER? OR COCYPHER? OR COCIPHER? OR CO-
             ENCRYPT? OR COINCOD? OR COENCOD?
S7          5   CO()(ENCIPHER? OR ENCYPHER? OR ENCOD??? ? OR INCOD??? ? OR
             ENCRYPT?)
S8     359258   VARIABLE? ?
S9       3793   S8(3N)(ADD OR ADDS OR ADDED OR ADDING OR ADDITIONAL OR SUP-
             PLEMENT? OR EXTRA OR AUXILIAR? OR ANCILL? OR ANOTHER OR AUGME-
             NT?)
S10     59403   (PARAMETER? OR PARAMETRE? OR VALUE OR VALUES OR NUMBER? ? -
             OR NUMERIC? OR NUMERAL? OR ALPHANUMERIC?)(2N)(CHANGEAB? OR CH-
             ANG??? ? OR VARY? OR VARIE? ? OR INCONSTAN? OR INDETERMINAT?)
S11      3332   (PARAMETER? OR PARAMETRE? OR VALUE OR VALUES OR NUMBER? ? -
             OR NUMERIC? OR NUMERAL? OR ALPHANUMERIC?)(2N)(UNFIX?? ? OR DY-
             NAMIC?)
S12       631   S10:S11(3N)(ADD OR ADDS OR ADDED OR ADDING OR ADDITIONAL OR
              SUPPLEMENT? OR EXTRA OR AUXILIAR? OR ANCILL? OR ANOTHER OR A-
             UGMENT?)
S13      3610   (FURTHER OR SECOND OR PAIR?? ?)(1W)S8
S14       111   S1:S5 AND (S6:S7 OR S9 OR S12)
S15      1317   S1:S5 AND S10:S11
S16        52   S1:S5 AND S13
S17    187542   ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR ENCOD???? ? OR INCOD-
             ???? ?
S18         5   S14 AND S17
S19        39   S15 AND S17
S20         1   S16 AND S17
S21     30923   IC='H04L-009'
S22     10581   IC='G09C-001'
S23        56   S14:S16 AND S21:S22
S24      8689   MC='W01-A05B'
S25      2055   MC='W01-C02B6A'
S26      4126   MC='W01-A05'
S27       196   MC='W01-C07A3'
S28      2557   MC='W02-L'
S29      1013   MC='W01-C08F'
S30        23   S14:S16 AND S24:S29
S31        83   S18:S20 OR S23 OR S30
S32        83   IDPAT (sorted in duplicate/non-duplicate order)
S33        83   IDPAT (primary/non-duplicate records only)
S34        81   S33 NOT (PROTEIN? OR DIODE? OR DNA)
S35        81   S34 NOT (POLYPEPTIDE? OR GENE? ? OR ACID? ? OR CDNA)
? t35/9/1,3,6,8-9,11,14-15,24,26,30-32,36
```

35/9/1   (Item 1 from file: 347)

DIALOG(R)File 347:JAPIO

07740830 **Image available**
EFFICIENT PACKET **ENCRYPTION** METHOD

PUB. NO.: 2003-234732 [JP 2003234732 A]
PUBLISHED: August 22, 2003 (20030822)
INVENTOR(s): GARSTIN MARK
GILMAN ROBERT R
ROBINSON RICHARD L
SIDDIQUI ANWAR
WUTZKE MARK
APPLICANT(s): AVAYA TECHNOLOGY CORP
APPL. NO.: 2002-382422 [JP 2002382422]
FILED: December 27, 2002 (20021227)
PRIORITY: 02 038295 [US 200238295], US (United States of America), January 04, 2002 (20020104)
INTL CLASS: **H04L-009/12** ; **H04L-009/36**

ABSTRACT

PROBLEM TO BE SOLVED: To provide an efficient packet **encryption** key in which the computation time for **encryption** /decryption is decreased and even when a packet is lost or the like, it can be recovered.
SOLUTION: This method comprises a step for generating an S-vector, a step for setting a **sequence number** , a step for setting a first variable, a step for setting a **second variable** , a step for setting a byte **sequence number** , a step for calculating a third variable from the **second variable** and the byte **sequence number** , a step for incrementing the byte **sequence number** , a step for calculating a fourth **variable** by **adding** the first **variable** to the value within the S-vector by the third variable, a step for locating an **encryption** byte and also a step for taking the exclusive ORing to generate the byte based on the third variable and the value within the S-vector by the fourth variable.

35/9/3 (Item 3 from file: 347)
DIALOG(R)File 347:JAPIO

07597659 **Image available**
INFORMATION SUPPLY DEVICE AND METHOD, AND METHOD FOR AUTHENTICATION USER FOR INFORMATION SUPPLY SYSTEM

PUB. NO.: 2003-091505 [JP 2003091505 A]
PUBLISHED: March 28, 2003 (20030328)
INVENTOR(s): TADA MASAO
APPLICANT(s): HITACHI LTD
APPL. NO.: 2001-282548 [JP 2001282548]
FILED: September 18, 2001 (20010918)
INTL CLASS: G06F-015/00; **H04L-009/32** ; H04N-001/32; H04N-001/44

ABSTRACT

PROBLEM TO BE SOLVED: To provide a FAX information supply device that can prevent others from knowing the entirety of a **password** at a time, make it more difficult for others to know the **password** and also enable a normal user to know unauthorized use of services by others when the others use the services unjustly.

SOLUTION: A **password** used by a user for an access to an information supply system comprises a fixed portion at which the user inputs the same value every time the user accesses and a variable portion at which the user inputs a **value** **varying** every time the user accesses. A second portion of a **password** which will be used by the user for a next access to the information supply device is generated, and both the second portion thus generated and supply information are transmitted to the user.

35/9/6 (Item 6 from file: 347)
DIALOG(R)File 347:JAPIO

07110262 **Image available**
DYNAMIC **PASSWORD** CONTROL SYSTEM

```
PUB. NO.:       2001-337929  [JP 2001337929  A]
PUBLISHED:      December 07, 2001 (20011207)
INVENTOR(s):    TAKAHASHI SHUICHI
APPLICANT(s):   NEC CORP
APPL. NO.:      2000-157136  [JP 2000157136]
FILED:          May 26, 2000 (20000526)
INTL CLASS:     G06F-015/00; G06F-017/60; G06K-017/00; G07D-009/00;
                H04L-009/32
```

ABSTRACT

PROBLEM TO BE SOLVED: To provide a dynamic **password** control system conducting an authentication process for a user by using a **password** having a **dynamically changed value** time-wise and not known to third persons easily.

SOLUTION: This dynamic **password** control system is provided with a stationary user terminal, an authentication server connected via a communication network, and a portable **password** calculating device. The stationary user terminal transmits a card ID, and the authentication server receiving the card ID calculates the dynamic **password** dynamically changed according to the elapsed time based on the **password** parameter inherent to the card ID and the elapsed time to determine the present **password** corresponding to the card ID. The portable **password** calculating device calculates the dynamic **password** by the same calculation logic as the authentication server to determine the present **password** when the elapsed time is inputted.

35/9/8 (Item 8 from file: 347)
DIALOG(R)File 347:JAPIO

06949967 **Image available**
TERMINAL AUTHENTICATION SYSTEM BY **DYNAMICALLY** VARIABLE **AUTHENTICATION NUMBER** GENERATING METHOD

```
PUB. NO.:       2001-177519  [JP 2001177519  A]
PUBLISHED:      June 29, 2001 (20010629)
INVENTOR(s):    GOHARA KEIJI
```

KITAGAWA TAKATSUNA
TOYOOKA HIROAKI
MATSUMOTO MITSUYOSHI
APPLICANT(s): HITACHI LTD
APPL. NO.: 11-358530 [JP 99358530]
FILED: December 17, 1999 (19991217)
INTL CLASS: **H04L-009/32** ; **G09C-001/00** ; **H04L-009/26**

ABSTRACT

PROBLEM TO BE SOLVED: To make it difficult to solve an authentication system even from an **authentication number** string exchanged between an authentication device and a device to be authenticated and also to make it difficult to forge the device to be authenticated.
SOLUTION: The device to be authenticated and the authenticating device hold a near **authentication number** (**authentication number** subset) of a plurality of times which makes an authentication success about the device to be authenticated, the device to be authenticated calculates a new aperiodic **authentication number** on the basis of the **authentication number** subset of the device to be authenticated by a function composed of a plurality of terms with which an aperiodic progression allocated to the device to be authenticated is obtained, the newly calculated **authentication number** is transmitted to the authenticating device, the authenticating device also calculates a new aperiodic **authentication number** by the function composed of the plurality of terms with which the aperiodic progression allocated to the device to be authenticated is obtained on the basis of the **authentication number** subset of the device to be authenticated, and the device to be authenticated is authenticated as proper in such a manner that the calculation result of the authentication device coincide with the **authentication number** transmitted from the device to be authenticated.

35/9/9 (Item 9 from file: 347)
DIALOG(R)File 347:JAPIO

06801100 **Image available**
METHOD AND DEVICE FOR TRANSMITTING DATA

PUB. NO.: 2001-028583 [JP 2001028583 A]
PUBLISHED: January 30, 2001 (20010130)
INVENTOR(s): KONDO KIYOMI
APPLICANT(s): NEC IC MICROCOMPUT SYST LTD
APPL. NO.: 11-200812 [JP 99200812]
FILED: July 14, 1999 (19990714)
INTL CLASS: **H04L-009/32** ; E05B-049/00; H04Q-009/00

ABSTRACT

PROBLEM TO BE SOLVED: To make theft of a device difficult by simple arithmetic by **enciphering** a transmission code with divided **ID codes** and an additional code.

SOLUTION: A code storage area 2 of a transmitter 1 for keyless entry is provided with an **ID code** storage area 3, where write is disabled except for special timing, a rolling code storage area 4 to add '1' each time of keying and an additional code area 5 for storing codes to be added to both the **enciphered ID code** and the rolling code. Concerning the codes stored in the storage areas, a processor group 6 has a function for

dividing the **ID code** , the rolling code and the additional code, a function for calculating the transmission start position of the **ID code** from the value of the rolling code and a function for **changing** the **number** of **additional** codes which correspond to the value of the divided additional code shown by the value of the rolling code. Then, the transmission code is **enciphered** by the divided **ID codes** and the additional codes.

35/9/11 (Item 11 from file: 347)
DIALOG(R)File 347:JAPIO

06396696 **Image available**
CIPHER KEY FORMATION AND **ENCRYPTION** METHOD

PUB. NO.: 11-338347 [JP 11338347 A]
PUBLISHED: December 10, 1999 (19991210)
INVENTOR(s): TSUKAMOTO KEIICHI
APPLICANT(s): HITACHI SOFTWARE ENG CO LTD
APPL. NO.: 10-149024 [JP 98149024]
FILED: May 29, 1998 (19980529)
INTL CLASS: **G09C-001/00** ; **G09C-001/00** ; G06F-007/58; **H04L-009/08**

ABSTRACT

PROBLEM TO BE SOLVED: To make illicit decipherment difficult and to make the high-speed processing with an electronic computer possible by forming two pseudo-random **number sequences** , **changing** the sequence of the one pseudo-random **number sequence** in accordance with the value of another pseudo-random **number sequence** and outputting the pseudo- random **number sequence** after a sequence change as a cipher key.

SOLUTION: The pseudo-random number RF is set at RX=RX0 for the purpose of initialization. The pseudo-random number RX is stored in an array element V[0] and a subscript I for storing the pseudo-random number RX formed in the subsequent processing into the array V is initialized to I=1 (S402, S403). The next pseudo-random number RX is calculated and is stored in the array element V[I] of the subscript I and further the subscript I of the array V for assigning the array element for storing the pseudo-random number RX to be calculated next is added (S404 to S406). A pointer P is positioned at the word at the top of plaintext/ciphertext data and the first/second pseudo-random number are calculated (S409). Next, the processing to obtain the agitation random numbers agitating the first pseudo-random **number sequence** is executed and Bellman processing is executed with the fetched pseudo-random number Rn as a key.

35/9/14 (Item 14 from file: 347)
DIALOG(R)File 347:JAPIO

05778177 **Image available**
REMOTE CONTROL DEVICE

PUB. NO.: 10-061277 [JP 10061277 A]
PUBLISHED: March 03, 1998 (19980303)

INVENTOR(s): NAKANO AKIO
APPLICANT(s): DENSO CORP [000426] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 08-222044 [JP 96222044]
FILED: August 23, 1996 (19960823)
INTL CLASS: [6] E05B-049/00; B60R-025/00; E05B-047/00; E05B-065/19; E05B-065/20; H04Q-009/00; H04Q-009/00
JAPIO CLASS: 31.9 (PACKAGING -- Other); 22.3 (MACHINERY -- Control & Regulation); 26.2 (TRANSPORTATION -- Motor Vehicles); 44.1 (COMMUNICATION -- Transmission Circuits & Antennae)
JAPIO KEYWORD:R131 (INFORMATION PROCESSING -- Microcomputers & Microprocessers)

ABSTRACT

PROBLEM TO BE SOLVED: To prevent illegal use by any one other than a user, by changing rolling codes on the basis of a key code to **encoded** rolling codes and **encoding ID codes** by use thereof.

SOLUTION: The exclusive logical sum of the constant X(sub 1) of x(sub 1) lot **number** in the **changed** table of rolling code and the rolling code A is operated. Next, a well-known M-series operation is carries out. Thereafter, the operation of exclusive logical sum by use of the constant code X after the x lot number and the M-series calculation are repeated n-times to **encode** the rolling code A and produce an **encoded** rolling code. And since the key code is written in the production process of vehicles, the key code is kept secret until the production process. Or if the key code is set at random in the production, even time designer who has contrived the logic can not decipher the **encode** of the rolling code A.

35/9/15 (Item 15 from file: 347)
DIALOG(R)File 347:JAPIO

05739894 **Image available**
CIPHERING DEVICE, DECIPHERING DEVICE, CIPHERING METHOD, DECIPHERING METHOD AND COMMUNICATION SYSTEM USING THE SAME

PUB. NO.: 10-022994 [JP 10022994 A]
PUBLISHED: January 23, 1998 (19980123)
INVENTOR(s): KOIDE AYUMI
TAKARAGI KAZUO
APPLICANT(s): HITACHI LTD [000510] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 08-175043 [JP 96175043]
FILED: July 04, 1996 (19960704)
INTL CLASS: [6] **H04L-009/20** ; **G09C-001/00** ; H04Q-007/38; **H04L-009/12** ; **H04L-009/16**
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 44.2 (COMMUNICATION -- Transmission Systems); 44.4 (COMMUNICATION -- Telephone); 44.9 (COMMUNICATION -- Other); 45.9 (INFORMATION PROCESSING -- Other)

ABSTRACT

PROBLEM TO BE SOLVED: To make decoding difficult and to securely synchronize **passwords** by generating a **password** key based on information which is set at every connection of a communication line between a base station and a moving station.

SOLUTION: Ciphering is executed by using the key generated in a key

generation part 200. The key generation part generates the **password** key based on information or the like which are set every time when the communication line is connected between the base station and the moving station. The **password** keys taking **dynamic values** different in every communication connection or every arbitrary time are made by generating the key from information. Random numbers outputted from a random number generation circuit part 202 are fed back and used as initial values for generating the next random numbers. The generated random numbers and data to be transmitted are operated in an exclusive OR operation part 203 and a **password** sentence of generated.

35/9/24 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

015899096 **Image available**
WPI Acc No: 2004-056935/200406
XRPX Acc No: N04-046036

Card authentication method e.g. for integrated circuit card, involves comparing fixed PIN **code and variable** authentication number **stored in card and controller, based on which card is authenticated**

Patent Assignee: MATSUSHITA ELECTRIC WORKS LTD (MATW)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2003346097	A	20031205	JP 2002154327	A	20020528	200406	B

Priority Applications (No Type Date): JP 2002154327 A 20020528
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2003346097	A		6	G06K-017/00	

Abstract (Basic): JP 2003346097 A

NOVELTY - An overwriting unit (4) overwrites **authentication number varying** according to authentication frequency of the card, in respective recording areas (6,7) of a card (3) and a controller (1), during card authentication. An authentication unit (5) compares fixed **PIN** code and **authentication number** recorded in card and controller, and authenticates the card if the compared numbers are in agreement with each other.

USE - For authenticating cards such as integrated circuit (IC) card and magnetic card.

ADVANTAGE - Prevents unauthorized access of the card, while allowing to know the access frequency of the card at the time of authentication, hence ensures security effectively.

DESCRIPTION OF DRAWING(S) - The figure shows a block diagram explaining the card authentication process. (Drawing includes non-English language text).

controller (1)
card (3)
authentication number overwriting unit (4)
authentication unit (5)
recording areas of card and controller (6,7)
pp; 6 DwgNo 1/3

Title Terms: CARD; AUTHENTICITY; METHOD; INTEGRATE; CIRCUIT; CARD; COMPARE; FIX; **PIN** ; CODE; VARIABLE; AUTHENTICITY; NUMBER; STORAGE; CARD; CONTROL; BASED; CARD; AUTHENTICITY
Derwent Class: Q47; T01; T04; T05; W01
International Patent Class (Main): G06K-017/00

```
International Patent Class (Additional): E05B-049/00; G06F-015/00;
  H04L-009/32
File Segment: EPI; EngPI
Manual Codes (EPI/S-X): T01-E04; T01-H01B3A; T01-H01C2; T01-H05B1;
  T01-N02B1B; T04-K02; T05-H02C5A; T05-H02C5C; T05-L01B; T05-L01X;
  W01-A05B


 35/9/26     (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004  Thomson Derwent. All rts. reserv.

015787794    **Image available**
WPI Acc No: 2003-849997/200379
  Pseudo-random generator and method using block  password  having spn
  structure
Patent Assignee: ELECTRONICS & TELECOM RES INST (ELTE-N)
Inventor: HONG D W; JANG G Y; JUNG B E; JUNG G I; KANG J S; KIM G U; RYU H
  S; SEO C H; SHIN S U; SONG J H
Number of Countries: 001  Number of Patents: 001
Patent Family:
Patent No     Kind   Date    Applicat No    Kind   Date     Week
KR 2003059500  A   20030710  KR 200188363    A   20011229  200379  B

Priority Applications (No Type Date): KR 200188363 A 20011229
Patent Details:
Patent No  Kind Lan Pg   Main IPC     Filing Notes
KR 2003059500 A      1 H04L-009/06

Abstract (Basic): KR 2003059500 A
        NOVELTY - A pseudo-random generator using a block  password  having
    an SPN structure and a method thereof are provided to improve a
    stability side by  changing  a key  value  through an update algorithm
    each time a random is generated.
        DETAILED DESCRIPTION - A reseeding module(102) collects a noise
    suited to each platform. The reseeding module(102) generates a key
    value based on noise information. The key value is used as an input of
    a random function. A pseudo-random generating module(104) includes two
    random function value converters. The pseudo-random generating
    module(104) uses the key value and a state value as inputs of the first
    random function value converter to generate the first random function
    value. The pseudo-random generating module(104) uses the first random
    function value and the key value as inputs of the second random
    function value converter to generate the first random function value to
    generate the second random function value. The pseudo-random generating
    module(104) outputs the second random function value as a pseudo-random
    value.
        pp; 1 DwgNo 1/10
Title Terms: PSEUDO; RANDOM; GENERATOR; METHOD; BLOCK;  PASSWORD ;
  STRUCTURE
Derwent Class: W01
International Patent Class (Main):  H04L-009/06
File Segment: EPI
Manual Codes (EPI/S-X): W01-A05A


 35/9/30     (Item 7 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004  Thomson Derwent. All rts. reserv.
```

```
015573359     **Image available**
WPI Acc No: 2003-635516/200360
XRPX Acc No: N03-505479
   Authentication   code  generation method for information access
  management, involves retrieving initial generation value of previous
  codes to obtain  PIN  and combining stored secret with generation value
Patent Assignee: BRAINARD J G (BRAI-I); KALISKI B S (KALI-I); RIVEST R L
  (RIVE-I)
Inventor: BRAINARD J G; KALISKI B S; RIVEST R L
Number of Countries: 001  Number of Patents: 001
Patent Family:
Patent No      Kind   Date     Applicat No    Kind   Date      Week
US 20030105964  A1  20030605  US 200110769    A   20011204  200360  B

Priority Applications (No Type Date): US 200110769 A 20011204
Patent Details:
Patent No  Kind Lan Pg   Main IPC    Filing Notes
US 20030105964 A1    18 H04L-009/00

Abstract (Basic): US 20030105964 A1
        NOVELTY - A  dynamic   value  associated with a time interval is
    determined. An initial generation value indicating the number of
    previous  authentication   code  generation is retrieved to define
    personal  identification   number  ( PIN ). An  authentication   code
    is generated by combining the stored secret,  dynamic  generation
    value  and the  PIN .
        DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for
    authentication   code  generating system.
        USE - For generating user  authentication   codes  while accessing
    information related to financial and health services through desktop
    computer, laptop computer and personal digital assistant (PDA).
        ADVANTAGE - Prevents risk of unauthorized access completely as the
    multi generation values are defined periodically and hence reliable
    secrecy is maintained during code generation.
        DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of
    authentication   code  generation system.
        pp; 18 DwgNo 2/4
Title Terms: AUTHENTICITY; CODE; GENERATE; METHOD; INFORMATION; ACCESS;
  MANAGEMENT; RETRIEVAL; INITIAL; GENERATE; VALUE; CODE; OBTAIN;  PIN ;
  COMBINATION; STORAGE; SECRET; GENERATE; VALUE
Derwent Class: T01; W01
International Patent Class (Main):  H04L-009/00
File Segment: EPI
Manual Codes (EPI/S-X): T01-D01; T01-E04; T01-J06A1; T01-N01A1; T01-N02B1B;
  W01-A05A;  W01-A05B


 35/9/31     (Item 8 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004  Thomson Derwent. All rts. reserv.

015480594
WPI Acc No: 2003-542741/200352
XRPX Acc No: N03-430502
   Encryption  method and device
Patent Assignee: QI Y (QIYY-I)
Inventor: QI Y
Number of Countries: 001  Number of Patents: 001
Patent Family:
Patent No      Kind   Date     Applicat No    Kind   Date      Week
```

```
CN 1416237     A   20030507  CN 2002139458   A   20021001  200352  B
```

Priority Applications (No Type Date): CN 2002139458 A 20021001
Patent Details:

```
Patent No  Kind Lan Pg   Main IPC     Filing Notes
CN 1416237    A        H04L-009/28
```

Abstract (Basic): CN 1416237 A

NOVELTY - The cipher code and the cipher text in the **enciphering** system are obtained through the corresponding data of the **dynamic** time **parameter** and the **dynamic sequence number parameters** , by combining specific cipher code and using the **enciphering** algorithm. The said corresponding data of the **dynamic** time **parameter** and the **dynamic sequence number parameter** are generated automatically in the system, and obtained at the moment when the relevant event of the **enciphered** object occurs. The method is suitable for the electronic file to generate the cipher code and the cipher test, for use of the electronicsignature and the electronic stamp to signl the e-text contract, the electronic bill as well as the anti-fraud of the products using the cipher code.

DwgNo 0/0

Title Terms: **ENCRYPTION** ; METHOD; DEVICE
Derwent Class: W01
International Patent Class (Main): **H04L-009/28**
International Patent Class (Additional): **H04L-009/00** ; **H04L-009/14**
File Segment: EPI
Manual Codes (EPI/S-X): **W01-A05** ; W01-A05A

35/9/32 (Item 9 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015393215
WPI Acc No: 2003-455356/200343

Method for generating random number for subscriber authentication in wireless communication system

Patent Assignee: ELECTRONICS & TELECOM RES INST (ELTE-N)
Inventor: HONG D W; JUNG B E; LEE O Y
Number of Countries: 001 Number of Patents: 001
Patent Family:

```
Patent No      Kind   Date     Applicat No     Kind   Date      Week
KR 2003014510  A    20030219  KR 200148538     A    20010811  200343  B
```

Priority Applications (No Type Date): KR 200148538 A 20010811
Patent Details:

```
Patent No  Kind Lan Pg   Main IPC     Filing Notes
KR 2003014510 A      1 H04L-009/22
```

Abstract (Basic): KR 2003014510 A

NOVELTY - A method for generating random number for subscriber authentication in wireless communication system is provided to generate a random number for a subscriber authentication which is used in a subscriber authentication and decoding/integrity key in order to serve an information security in a core network authentication center of a wireless communication system.

DETAILED DESCRIPTION - An internal state value and a user **password** key are calculated by a CASUMI method. A **change value** of the internal state value and the user **password** key and an operator key are operated by an XOR and KASUMI method. Data according to the XOR and

KASUMI-operation and the user **password** key and a random number constant value are operated by an XOR and KASUMI method to generate a random number row. Data according to the KASUMI-operation and the data according to the XOR and KASUMI-operation, and the operator key are operated by XOR and KASUMI method to determine the result as the random number constant value.

pp; 1 DwgNo 0/10

Title Terms: METHOD; GENERATE; RANDOM; NUMBER; SUBSCRIBER; AUTHENTICITY; WIRELESS; COMMUNICATE; SYSTEM
Derwent Class: W01; W02
International Patent Class (Main): **H04L-009/22**
File Segment: EPI
Manual Codes (EPI/S-X): W01-A05A; W02-C01B1

35/9/36 (Item 13 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

014612942 **Image available**
WPI Acc No: 2002-433646/200246
XRPX Acc No: N02-341212

Password **protected computer system access permission method involves permitting user to access computer only, when internal hash value is equal to external has value**

Patent Assignee: COMPAQ COMPUTER CORP (COPQ)
Inventor: ANGELO M F; HEINRICH D F; LE H Q; WALDORF R O
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6370649	B1	20020409	US 9833192	A	19980302	200246	B

Priority Applications (No Type Date): US 9833192 A 19980302
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6370649	B1		13	H04K-001/00	

Abstract (Basic): US 6370649 B1

NOVELTY - A internal hash value, generated is based on a **changeable** seed **value** distinct from a previous fail safe **password** . The fail safe **password** is decrypted using a public key corresponding to private key to provide an external hash value. The user is permitted to access the computer system only when the internal and external hash values are equal.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for a computer system.

USE - For allowing a user to access a **password** protected computer system.

ADVANTAGE - Allows a manufacturer to securely supply a single use **password** to users who lose or misplace a system **password** . Provides a hardened **password** security infrastructure that discourages theft of computer effectively.

DESCRIPTION OF DRAWING(S) - The figure shows the flowchart illustrating a procedure for verifying a **password** upon power-up of the computer system.

pp; 13 DwgNo 2A/5

Title Terms: **PASSWORD** ; PROTECT; COMPUTER; SYSTEM; ACCESS; PERMIT; METHOD; PERMIT; USER; ACCESS; COMPUTER; INTERNAL; HASH; VALUE; EQUAL; EXTERNAL; VALUE
Derwent Class: T01; W01

International Patent Class (Main): H04K-001/00
File Segment: EPI
Manual Codes (EPI/S-X): T01-D01; T01-H01C2; T01-J12C; **W01-A05B**
? t35/9/40-42,44,48,62,65,70-72,75

35/9/40 (Item 17 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

014143604
WPI Acc No: 2001-627815/200173
XRPX Acc No: N01-468139
Releasing a coded data file involves the use of equipment identifiers established by using enciphered **codes and keys passed between a local computer system and a central station**
Patent Assignee: MANNESMANN VDO AG (MANS); DRIJFHOUT T (DRIJ-I); THOONE M (THOO-I)
Inventor: DRIJFHOUT T; THOONE M
Number of Countries: 028 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1139196	A1	20011004	EP 2000106809	A	20000330	200173	B
AU 200128029	A	20011004	AU 200128029	A	20010315	200173	
US 20010047341	A1	20011129	US 2001823875	A	20010330	200202	
CN 1315716	A	20011003	CN 2001112437	A	20010330	200205	

Priority Applications (No Type Date): EP 2000106809 A 20000330
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1139196	A1	G	16	G06F-001/00	

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
AU 200128029	A			G06F-012/14	
US 20010047341	A1			G06F-017/60	
CN 1315716	A			G06K-019/073	

Abstract (Basic): EP 1139196 A1

NOVELTY - The method involves passing an equipment identifier from a local computer system to a central station, computing a new equipment identifier using a change code, specifying a first **enciphered** code using a key, specifying a second **enciphered** code using the data file identifier, passing the **enciphered** codes to the local system, computing the new equipment identifier, the key and data file identifier in the local system and releasing the data file.

DETAILED DESCRIPTION - The method involves passing an equipment identifier (ID(i-1)) from a local computer system to a central station, computing a new equipment identifier (ID(i)) from the equipment **number** and a **change** code, specifying a first **enciphered** code (**PIN**) using the computed code and a key (k), specifying a second **enciphered** code (ACW) using the data file identifier and the key, passing the **enciphered** codes to the local system, computing the new equipment identifier in the local system from the stored identifier and the change code, computing the key from the first **enciphered** code and the equipment identifier, computing the data file identifier (AC) from the second **enciphered** code and the key and releasing the data file for use by the local system. INDEPENDENT CLAIMS are also included for the following: a system for managing and releasing access rights to data files.

USE - For managing and releasing access rights to data files form use by only one or a limited number of local computer systems.

ADVANTAGE - Ensures that a computer program or data file is only accessed by an authorized user and enables the release of only single programs or data files for a defined user.

pp; 16 DwgNo 0/5

Title Terms: RELEASE; CODE; DATA; FILE; EQUIPMENT; IDENTIFY; ESTABLISH; **ENCIPHER** ; CODE; KEY; PASS; LOCAL; COMPUTER; SYSTEM; CENTRAL; STATION
Derwent Class: T01
International Patent Class (Main): G06F-001/00; G06F-012/14; G06F-017/60; G06K-019/073
International Patent Class (Additional): G06F-009/06; G06F-012/00; G06F-013/00; G06F-017/30; **H04L-009/28**
File Segment: EPI
Manual Codes (EPI/S-X): T01-D01; T01-H07C3; T01-H07C5C; T01-H07C5E; T01-H07C5S; T01-J12C

35/9/41 (Item 18 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

013839844 **Image available**
WPI Acc No: 2001-324057/200134
XRPX Acc No: N01-233624
Packet communication system for stream encryption **system, has** encryption **key setting unit by which** encryption **key for every packet is changed using dummy random** number sequence
Patent Assignee: TOYO COMMUNICATION EQUIP CO (TOCM)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2001086110	A	20010330	JP 99258447	A	19990913	200134	B

Priority Applications (No Type Date): JP 99258447 A 19990913
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2001086110	A		7	H04L-009/18	

Abstract (Basic): JP 2001086110 A

NOVELTY - A packet generator (11) generates several data packets. An **encryption** key setting unit (13) generates dummy random **number sequence** to **change** the **encryption** key for every packet as its initial value. A stream **encryption** unit (12) performs **encryption** of portion of packet information using binary dummy random **number sequence** .

DETAILED DESCRIPTION - A key storing unit (14) stores the **encryption** key information as a part of packet information. A packet transmitting unit (15) sequentially transmits the packets each consisting data portion and **encryption** key information.

USE - For stream **encryption** system.

ADVANTAGE - Synchronization of **encryption** key modification is not needed for the **encryption** key modification. Hence, problem due to the slippage of synchronization and hardware loading are avoided.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of the packet transmission device. (Drawing includes non-English language text).

Packet generator (11)
Stream **encryption** unit (12)
Encryption key setting unit (13)
Key storing unit (14)
Packet transmitting unit (15)

```
        pp; 7 DwgNo 1/9
Title Terms: PACKET; COMMUNICATE; SYSTEM; STREAM;  ENCRYPTION ; SYSTEM;
  ENCRYPTION ; KEY; SET; UNIT;  ENCRYPTION ; KEY; PACKET; CHANGE; DUMMY;
  RANDOM; NUMBER; SEQUENCE
Derwent Class: W01
International Patent Class (Main):  H04L-009/18
International Patent Class (Additional):  H04L-009/08 ; H04L-012/56
File Segment: EPI
Manual Codes (EPI/S-X): W01-A03B


 35/9/42     (Item 19 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004  Thomson Derwent. All rts. reserv.

013797259     **Image available**
WPI Acc No: 2001-281471/200129
XRPX Acc No: N01-200727
   Password  disclosing method in selective call device, involves receiving
  timed input to  vary  preset  value  representing specific time period,
  and presenting secured  password  when the value reaches a threshold
Patent Assignee: MOTOROLA INC (MOTI  )
Inventor: HYMEL J A
Number of Countries: 023  Number of Patents: 001
Patent Family:
Patent No     Kind   Date    Applicat No    Kind   Date     Week
WO 200119064    A1  20010315  WO 2000US23109  A   20000823  200129  B

Priority Applications (No Type Date): US 99393283 A 19990910
Patent Details:
Patent No  Kind Lan Pg   Main IPC    Filing Notes
WO 200119064  A1 E  17 H04M-011/00
   Designated States (National): BR CN JP KR MX
   Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU
   MC NL PT SE
Abstract (Basic): WO 200119064 A1
        NOVELTY - The method involves storing a secured  password  and
    preset value representative of a period of time. A timed input is
    received, and the preset  value  is  varied  in response to the timed
    input. The secured  password  is presented in response to the preset
    value reaching a threshold value.
        USE - For disclosing  password  in selective calling device.
        ADVANTAGE - Prevents users of discounted selective call devices
    from changing service providers during the contract period. Provides
    users of the selective call device with the option or freedom to change
    services if they desire at the end of the contract period.
        DESCRIPTION OF DRAWING(S) - The figure shows the electrical block
    diagram of selective call device employee  password  disclosing method.

        pp; 17 DwgNo 2/4
Title Terms:  PASSWORD ; DISCLOSE; METHOD; SELECT; CALL; DEVICE; RECEIVE;
  TIME; INPUT; VARY; PRESET; VALUE; REPRESENT; SPECIFIC; TIME; PERIOD;
  PRESENT; SECURE;  PASSWORD ; VALUE; REACH; THRESHOLD
Derwent Class: W01; W05
International Patent Class (Main): H04M-011/00
File Segment: EPI
Manual Codes (EPI/S-X): W01-C05A;  W01-C08F ; W05-A05C


 35/9/44     (Item 21 from file: 350)
```

```
DIALOG(R)File 350:Derwent WPIX
(c) 2004  Thomson Derwent. All rts. reserv.

013475767     **Image available**
WPI Acc No: 2000-647710/200063
XRPX Acc No: N01-005496
  Authenticating system for confirming user identity for carrying out
  transactions over Internet, uses dynamic personal identification
  number  ( PIN ) to provide improved security
Patent Assignee: LU T (LUTT-I)
Inventor: LU T
Number of Countries: 002  Number of Patents: 002
Patent Family:
Patent No      Kind   Date     Applicat No     Kind   Date      Week
CA 2291430      A1   20000728  CA 2291430       A    19991201  200063  B
CN 1268721      A    20001004  CN 2000102265    A    20000215  200067

Priority Applications (No Type Date): US 99336483 A 19990616; US 99117506 A
  19990128; CA 2267672 A 19990215
Patent Details:
Patent No  Kind Lan Pg   Main IPC     Filing Notes
CA 2291430    A1 E  48 H04L-009/32
CN 1268721    A        G06K-019/06
Abstract (Basic): CA 2291430 A1
        NOVELTY - A new dynamic  PIN  comprising an event identifier and a
    pseudo-random  number  sequence  identifier, is generated for each
    transaction, by a user card (12), by generating a distinct
    pseudo-random number based on a private seed and a previous random
    number stored by the user card and incrementing the value of the event
    identifier. The  PIN  is then transmitted to an authentication server
    (18) along with a preestablished user account name.
        DETAILED DESCRIPTION - The authentication server retrieves the
    private seed, and previous event and pseudo-random identifiers from a
    secure account database (20) associated with the account name. The
    authentication server ensures that the stored event identifier
    corresponds to the event identifier provided by the user by
    incrementing the event identifier if necessary and by generating a
    successive pseudorandom identifier each time the event identifier is
    incremented. Once the event identifiers correspond, the latest
    pseudo-random identifier is compared with the pseudo-random identifier
    transmitted by the user within the  PIN . If authentication is
    successful, the authentication server will then complete the financial
    transaction associated with the user's request.
        An INDEPENDENT CLAIM is also included for a method of
    authenticating identity of user.
        USE - For providing transactional security over Internet.
        ADVANTAGE - Provides simple, relatively inexpensive and easy to use
    transactional security system which does not transfer any sensitive
    data over Internet and which does not require installation of
    complicated software or hardware by either customer or merchant.
        DESCRIPTION OF DRAWING(S) - The drawing shows schematically the
    basic components of authenticating system for confirming identity of
    user.
        User card (12)
        Authentication server (18)
        Secure account database (20)
        pp; 48 DwgNo 1/10
Title Terms: AUTHENTICITY; SYSTEM; CONFIRM; USER; IDENTIFY; CARRY;
  TRANSACTION; DYNAMIC; PERSON; IDENTIFY; NUMBER;  PIN ; IMPROVE; SECURE
Derwent Class: T01; W01
```

International Patent Class (Main): G06K-019/06; **H04L-009/32**
International Patent Class (Additional): G06F-015/16; H04L-012/22
File Segment: EPI
Manual Codes (EPI/S-X): T01-E04; T01-H07C5E; T01-H07C5S; T01-J05A1;
T01-J12C; **W01-A05B** ; W01-A06B7; W01-A06E1A

35/9/48 (Item 25 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

012712845 **Image available**
WPI Acc No: 1999-518958/199943
XRPX Acc No: N99-385927
Service access protection method for telecommunication network - entering sequence **of** numbers **by user and adding further parameter to sequence before transmission through network to central instance for evaluation**
Patent Assignee: SIEMENS AG (SIEI)
Inventor: GUNDLACH M; NAUER B
Number of Countries: 021 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9944332	A1	19990902	WO 98DE2949	A	19981002	199943	B
BR 9815697	A	20001114	BR 9815697	A	19981002	200064	
			WO 98DE2949	A	19981002		
EP 1058982	A1	20001213	EP 98959711	A	19981002	200066	
			WO 98DE2949	A	19981002		
JP 2002505552	W	20020219	WO 98DE2949	A	19981002	200216	
			JP 2000533979	A	19981002		

Priority Applications (No Type Date): DE 1008523 A 19980227
Patent Details:

```
Patent No  Kind Lan Pg   Main IPC     Filing Notes
WO 9944332    A1 G  23 H04L-009/32
   Designated States (National): BR JP US
   Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU
   MC NL PT SE
BR 9815697    A         H04L-009/32   Based on patent WO 9944332
EP 1058982    A1 G      H04L-009/32   Based on patent WO 9944332
   Designated States (Regional): DE ES FR GB IT
JP 2002505552 W      19 H04L-009/32   Based on patent WO 9944332
```

Abstract (Basic): WO 9944332 A

The method involves entering a **number sequence** which is only known by the user of the service. The **number sequence** is transmitted transparently in the communication network via exchange nodes (SSP) to a service control point (SCP) at which the **number sequence** is evaluated. The **number sequence** is **supplemented** by a **changeable** further **parameter** before the transmission through the communication network.

The sequence is **encoded** using a mathematical algorithm. The result is transmitted to the service control point using multi-frequency dialling. An authentication is carried out in the service control point. Preferably, the telecommunication network is an intelligent network.

USE - E.g. for credit card calling.

ADVANTAGE - Provides better security against monitoring.

Dwg.1/3

Title Terms: SERVICE; ACCESS; PROTECT; METHOD; TELECOMMUNICATION; NETWORK;
ENTER; SEQUENCE; NUMBER; USER; ADD; PARAMETER; SEQUENCE; TRANSMISSION;

THROUGH; NETWORK; CENTRAL; INSTANCE; EVALUATE
Derwent Class: P85; W01
International Patent Class (Main): **H04L-009/32**
International Patent Class (Additional): G06F-015/00; **G09C-001/00** ; H04M-003/42; H04M-015/00
File Segment: EPI; EngPI
Manual Codes (EPI/S-X): **W01-A05B** ; W01-B09; W01-C02A7A; **W01-C02B6A** ; W01-C06; **W01-C07A3** ; **W01-C08F**

35/9/62 (Item 39 from file: 350)
DIALOG(R)File 350:Derwent WPIX

011075670 **Image available**
WPI Acc No: 1997-053594/199706
XRPX Acc No: N97-043898
Fraud-proof equipment identification method - using equipment number and time variable data part based on pseudorandom number derived from initial value **and** changed **by clock with clocking rate matched to shortest anticipated call-up sequence**
Patent Assignee: ALCATEL SEL AG (COGE)
Inventor: BEIER W
Number of Countries: 001 Number of Patents: 001
Patent Family:

```
Patent No     Kind   Date     Applicat No     Kind   Date      Week
DE 19523654    A1  19970102  DE 1023654        A   19950629  199706  B
```

Priority Applications (No Type Date): DE 1023654 A 19950629
Patent Details:

```
Patent No    Kind Lan Pg   Main IPC     Filing Notes
DE 19523654   A1      5 H04L-009/32
```

Abstract (Basic): DE 19523654 A

The method involves using an equipment number (10) and a time variable data part based on a pseudorandom number (P) which can be derived from an initial value in a predefined manner. The pseudorandom **number** is **changed** each time it is called up.

The pseudorandom **number** is **changed** by a clock, whose clocking rate is matched to the shortest anticipated call-up sequence, and is prepared with the equipment number for call-up. The pseudorandom number can be used as a key to **encode** the equipment number. It can also be extracted from a longer pseudorandom number.

ADVANTAGE - Increases security against cracking of **identification codes** .

Dwg.1/1

Title Terms: FRAUD; PROOF; EQUIPMENT; IDENTIFY; METHOD; EQUIPMENT; NUMBER; TIME; VARIABLE; DATA; PART; BASED; NUMBER; DERIVATIVE; INITIAL; VALUE; CHANGE; CLOCK; CLOCK; RATE; MATCH; SHORT; ANTICIPATE; CALL; UP; SEQUENCE
Derwent Class: W01; W02
International Patent Class (Main): **H04L-009/32**
International Patent Class (Additional): H04B-001/38; H04B-001/59
File Segment: EPI
Manual Codes (EPI/S-X): **W01-A05B** ; W01-C01D1D; W01-C01D3D; W02-G02C; W02-G05

35/9/65 (Item 42 from file: 350)
DIALOG(R)File 350:Derwent WPIX

010255544 **Image available**
WPI Acc No: 1995-156799/199521
XRPX Acc No: N95-123476

Electronic combination lock operated from separate computer system - has computer processor which executes series of steps to generates authorised combination which is compared with that input by user, and opens lock if match occurs

Patent Assignee: MAS-HAMILTON GROUP (MASH-N); MAS-HAMILTON GROUP INC (MASH-N); KABA MAS CORP (KABA-N)
Inventor: DAWSON G L; THOMPSON D L
Number of Countries: 008 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 649957	A2	19950426	EP 94307708	A	19941020	199521	B
CA 2133057	A	19950421	CA 2133057	A	19940927	199529	
US 5488660	A	19960130	US 93139450	A	19931020	199611	
			US 95416455	A	19950403		
EP 649957	A3	19950816	EP 94307708	A	19941020	199613	
US 37011	E	20010109	US 93139450	A	19931020	200104	
			US 95416455	A	19950403		
			US 97906535	A	19970805		
US 38147	E	20030617	US 93139450	A	19931020	200348	
			US 95416455	A	19950403		
			US 97906535	A	19970805		
			US 99419542	A	19991019		

Priority Applications (No Type Date): US 93139450 A 19931020; US 95416455 A 19950403; US 97906535 A 19970805; US 99419542 A 19991019
Cited Patents: EP 459781; EP 546701; US 5061923
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 649957	A2	E	20	E05B-049/00	
Designated States (Regional): CH DE FR GB IT LI					
CA 2133057	A			E05B-047/00	
US 5488660	A		18	H04K-001/00	Cont of application US 93139450
EP 649957	A3			E05B-049/00	
US 37011	E			H04K-001/00	CIP of application US 93139450 Reissue of patent US 5488660
US 38147	E			H04K-001/00	CIP of application US 93139450 Cont of application US 97906535 Cont of patent US 3701 Reissue of patent US 5488660

Abstract (Basic): EP 649957 A

The electronic combination lock has an input dial for entering combination numbers into the lock, and a display which indicates the numbers. An electronic controller receives combination sequences and compares them with the **authorised sequence** . The electronic controller has an **encryption** device which **encrypts** an input combination sequence, and generates a combination derived from the predetermined data. A comparator evaluates the entered combination with the generated combination, and generates an opening signal.

The **encryption** generator responds to the last accepted combination, a parameter unique to the lock, a master combination and a variable value. The variable **value** is **changed** in a predictable manner for each opening of the lock and the result is manipulated to generate the authorised combination.

USE/ADVANTAGE - E.g. for anti-theft device or secure container.Each new opening of lock requires new combination from computer.

Dwg.2/8

Abstract (Equivalent): US 5488660 A

An electronic combination lock comprising:

an input dial for inputting numbers of a combination into said lock;

a display for displaying numbers;

an electronic control means for receiving said numbers of said combinations and for comparing said numbers with numbers of an authorized combination;

said electronic control means including:

an **encrypting** combination generator responsive to an entered combination for **encrypting** predetermined data and for generating a combination derived from said predetermined data;

a comparator for comparing said entered combination with said generated combination and responsive to a compare equal to generate a signal permitting said lock to open,

said **encrypting** and generating means responsive to a last accepted combination, a parameter unique to said lock, a master combination, a variable value, said variable **value changed** in a predictable manner upon each opening of said lock to form a result and manipulation of said result, to generate said authorized combination.

Dwg.4/8

Title Terms: ELECTRONIC; COMBINATION; LOCK; OPERATE; SEPARATE; COMPUTER; SYSTEM; COMPUTER; PROCESSOR; EXECUTE; SERIES; STEP; GENERATE; AUTHORISE; COMBINATION; COMPARE; INPUT; USER; OPEN; LOCK; MATCH; OCCUR
Derwent Class: Q47; T01; T05; X25
International Patent Class (Main): E05B-047/00; E05B-049/00; H04K-001/00
International Patent Class (Additional): G06F-007/04; **H04L-009/00**
File Segment: EPI; EngPI
Manual Codes (EPI/S-X): T01-J08A; T01-S; T05-L03C; X25-M01

35/9/70 (Item 47 from file: 350)
DIALOG(R)File 350:Derwent WPIX

008851997 **Image available**
WPI Acc No: 1991-356017/199149
XRPX Acc No: N91-272471

Remote control device - performs encoding **function on** identification number **embedded in micro-chip and combination of unit and stepping counting numbers**

Patent Assignee: MICROCHIP TECHNOLOGY INC (MICR-N); NANOTEQ PTY LTD (NANO-N)
Inventor: BRUWER F J; KUEHN G J; SMIT W; KUHN G J
Number of Countries: 016 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 459781	A	19911204	EP 91304847	A	19910529	199149	B
ZA 9104063	A	19930331	ZA 914063	A	19910529	199319	
EP 459781	B1	19960417				199620	
US 5517187	A	19960514	US 91707101	A	19910529	199625	
			US 9319821	A	19930218		
DE 69118748	E	19960523	DE 618748	A	19910529	199626	
			EP 91304847	A	19910529		
ES 2085425	T3	19960601	EP 91304847	A	19910529	199629	
US 6175312	B1	20010116	US 91707101	A	19910529	200106	
			US 92985929	A	19921204		

Priority Applications (No Type Date): ZA 904088 A 19900529; ZA 922402 A 19920402
Cited Patents: DE 3532156; FR 2606232; FR 2607544; GB 2133073

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 459781	A				
Designated States (Regional): AT BE CH DE ES FR GB GR IT LI LU NL SE					
ZA 9104063	A		42	H04Q-000/00	
EP 459781	B1	E	21	E05B-049/00	
Designated States (Regional): AT BE CH DE DK ES FR GB GR IT LI LU NL SE					
US 5517187	A		16	H04Q-009/00	Cont of application US 91707101
DE 69118748	E			E05B-049/00	Based on patent EP 459781
ES 2085425	T3			E05B-049/00	Based on patent EP 459781
US 6175312	B1			H04Q-009/00	CIP of application US 91707101

Abstract (Basic): EP 459781 A

The **encoder** microchip comprises a non linear **encoding** unit for embedding an **encoded identification number** in the microchip and a combination of a unit number and a stepping counter value. This action generates a transmission value which is only decodable by a related decoding function having access to the same **identification number** . When a synchronisation command is given, a counter value is generated which is **encodable** together with the synchronisation command, to generate a sync. transmission value which will facilitate sync. of a related decoder microchip having the same **identification number** .

The decoder microchip performs a format scan on ten signals to identify and respond to valid transmission values.

ADVANTAGE - Increased security without reducing user friendliness.

(17pp Dwg.No.1/6

Abstract (Equivalent): EP 459781 B

An **encoder** for an access control system, comprising: means (6) for defining an **identification number** for an **encoding** operation; means (4, 5) for storing a counter value; means (7) for performing an **encoding** function using the **identification number** , on data comprising the counter value, to generate an **encoded** value therefrom which can be decoded by a related decoding function using a related **identification number** to yield the counter value; and means (2, 4) for **changing** the counter **value** in association with each operation of the **encoder** , to **vary** the **encoded value** independently of time.

(Dwg.1/6

Abstract (Equivalent): US 5517187 A

A system which includes an **encoder** microchip and a decoder microchip, wherein:

said **encoder** microchip comprises:

means for storing an **identification number** ,

means for storing a counter value,

means for **changing** the **value** of said counter value each time the **encoder** microchip is operated, and

encoding means for performing a nonlinear **encoding** function on said counter value using said **identif**ication number , so as to generate a transmission value;

said decoder microchip comprises:

means for storing a second **identification number** ,

means for receiving said transmission value from said **encoder** microchip,

means for performing a decoding function on said transmission value using said second **identification number** , so as to generate from said transmission value a decoded counter value,

means for storing a second decoded counter value obtained from the decoding of a transmission value of a previous transmission by said means for performing a decoding function; and

means for performing a format scan on signals so as to identify

signals conforming to a specific format.
(Dwg.1/6

Title Terms: REMOTE; CONTROL; DEVICE; PERFORMANCE; **ENCODE** ; FUNCTION; IDENTIFY; NUMBER; EMBED; MICRO; CHIP; COMBINATION; UNIT; STEP; COUNT; NUMBER
Derwent Class: Q47; U13; U21; W01; W05; X22
International Patent Class (Main): E05B-049/00; H04Q-000/00; H04Q-009/00
International Patent Class (Additional): G07F-007/00; G07F-007/10; G08C-000/00
File Segment: EPI; EngPI
Manual Codes (EPI/S-X): W05-C; W05-D04; X22-D

35/9/71 (Item 48 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

008793784 **Image available**
WPI Acc No: 1991-297798/199141
XRPX Acc No: N91-228178

Coded emitter for telephone based transactions - uses encoded **acoustic transmission over telephone system with** encoding **changing at each use of emitter**

Patent Assignee: BERNARD A (BERN-I)
Inventor: BERNARD A
Number of Countries: 016 Number of Patents: 008
Patent Family:

```
Patent No      Kind   Date     Applicat No     Kind   Date      Week
EP 451056       A   19911009  EP 91400915     A   19910404  199141  B
FR 2660776      A   19911011                                199151
US 5182767      A   19930126  US 91680551     A   19910404  199307
JP 6070048      A   19940311  JP 9199800      A   19910405  199415
EP 451056       B1  19950301  EP 91400915     A   19910404  199513
DE 69107652     E   19950406  DE 607652       A   19910404  199519
                              EP 91400915     A   19910404
ES 2071247      T3  19950616  EP 91400915     A   19910404  199531
JP 3009751      B2  20000214  JP 9199800      A   19910405  200013
```

Priority Applications (No Type Date): FR 904367 A 19900405
Cited Patents: 1.Jnl.Ref; EP 61373; JP 61043050
Patent Details:

```
Patent No  Kind Lan Pg   Main IPC     Filing Notes
EP 451056     A      7
   Designated States (Regional): AT BE CH DE ES FR GB GR IT LI LU NL SE
JP 3009751    B2     5 H04M-011/00   Previous Publ. patent JP 6070048
US 5182767    A      5 H04M-001/26
JP 6070048    A      7 H04M-011/00
EP 451056     B1 F   6 G07F-007/08
   Designated States (Regional): AT BE CH DE DK ES FR GB GR IT LI LU NL SE
DE 69107652   E        G07F-007/08   Based on patent EP 451056
ES 2071247    T3       G07F-007/08   Based on patent EP 451056
```

Abstract (Basic): EP 451056 A

The portable electronic unit has an acoustic emitter (10) and a driver (12) generating tones corresponding to keys on a telephone, and a circuit (34) that forms a digital message (M). The message generator has a memory (14) containing an **identification code** (N) and a key (C). The digital message changes at each use and is set by the values of the code and key.

A circuit (16) translates the number stream to signals that e control the tones delivered by the acoustic emitter.

ADVANTAGE - - Increased security against misuse in systems

allowing payment for services over telephone. (7pp Dwg.No.1/2

Abstract (Equivalent): EP 451056 B

Electronic telephone device including: an acoustic transmitter (10), a generator (12) for controlling an acoustic transmitter and able to generate tones falling within the telephone band, a device (34) able to form a digital message (M) formed of a set of **numbers changing** on each use of the device, said device comprising: a memory (14) containing a first **identification code** (N) and a second or service key (C) code linked to the telephone system in which the device is used and an electronic and logic circuit (16) connected to the memory (14) and delivering th message controlling the generator (12), this message depending on the firs and second codes, each number of the message controlling the generator (12) so as to have the acoustic transmitter (10) transmit a particular tone, this transmitter thus transmitting a sequence (SQ) of tones, a battery (27) for feeding the device (34) able to form the digital message (M), said device (34) being characterized in that the device able to form a digital message (M) comprises means producing an information making it possible to mark the instant where the device is time limited or scratched and to modify the **sequence** of **numbers** and in that it comprises a manually controlled switch (24) able to put into service the generator (12) in order to transmit the sequence of tones (SQ).

(Dwg.1/2

Abstract (Equivalent): US 5182767 A

The electronic telephone device comprises an acoustic transmitter and an acoustic generator controlling the acoustic transmitter and generating tones falling within the telephone band. A digital message which consists of a set of numbers is generated. The set of **numbers changes** on each use of the electronic device. The digital message generator determines a time limitation moment.

The digital message generator comprises a memory containing a first **identification code** and a second code of a service key linked to the telephone system in which the device is used. An electronic and logic circuit is connected to the memory, for delivering a message controlling the generator, this message depending on the two codes. Each number of the message controls the generator so as to have the acoustic transmitter transmit a partic. sequence of tones. A battery powers the device. A manually controlled switch puts the acoustic generator into service so as to transmit the sequence of tones.

ADVANTAGE - Has shape of token with switch on one side and loudspeaker on the other.

Dwg.1/2

Title Terms: CODE; EMITTER; TELEPHONE; BASED; TRANSACTION; **ENCODE** ; ACOUSTIC; TRANSMISSION; TELEPHONE; SYSTEM; **ENCODE** ; CHANGE; EMITTER

Derwent Class: T01; T05; W01

International Patent Class (Main): G07F-007/08; H04M-001/26; H04M-011/00

International Patent Class (Additional): G07C-009/00; G07F-001/06; G07F-017/28; **H04L-009/32** ; H04M-011/06

File Segment: EPI

Manual Codes (EPI/S-X): T01-J05A; T05-H02; T05-H05; T05-L; W01-C05B3

35/9/72 (Item 49 from file: 350)

DIALOG(R)File 350:Derwent WPIX

008660378 **Image available**

WPI Acc No: 1991-164405/199122

Related WPI Acc No: 1987-199010; 1988-036274; 1989-285598; 1991-087031; 1991-192862; 1992-167414

```
XRAM Acc No: C90-093768
XRPX Acc No: N91-125949
  System for secure identification and verification - uses coded active
  units with time varying code responding when in proximity to checkpoint
Patent Assignee: SECURITY DYNAMICS TECHN (SECU-N); SECURITIES DYNAMICS
   (SECU-N); US SEC OF INTERIOR (USSI  ); SECURITY DYNAMICS T (SECU-N)
Inventor: WEISS K P
Number of Countries: 018  Number of Patents: 014
Patent Family:
Patent No     Kind  Date    Applicat No    Kind   Date     Week
WO 9106926     A   19910516                                199122  B
AU 9067208     A   19910531                                199135
US 5058161     A   19911015  US 89429326     A   19891031  199144
US 5097505     A   19920317  US 90597784     A   19901019  199214
EP 497889      A1  19920812  EP 90916922     A   19901024  199233
                             WO 90US6079     A   19901024
US 7429326     N                                           199314
JP 5503598     W   19930610  JP 90515633     A   19901024  199328
                             WO 90US6079     A   19901024
EP 555219      A1  19930818  EP 91911098     A   19910430  199333
                             WO 91US3034     A   19910430
AU 642362      B   19931014  AU 9067208      A   19901024  199348
JP 6507277     W   19940811  JP 91510597     A   19910430  199436
                             WO 91US3034     A   19910430
EP 497889      B1  19951220  EP 90916922     A   19901024  199604
                             WO 90US6079     A   19901024
DE 69024367    E   19960201  DE 624367       A   19901024  199610
                             EP 90916922     A   19901024
                             WO 90US6079     A   19901024
ES 2084710     T3  19960516  EP 90916922     A   19901024  199627
CA 2072150     C   19971209  CA 2072150      A   19901024  199810

Priority Applications (No Type Date): US 90597784 A 19901019; US 89429326 A
  19891031; US 84676626 A 19841130; US 85802579 A 19851127; US 91670705 A
  19910318
Cited Patents: EP 131112; EP 178924; EP 301127; FR 2607544; FR 2616252; US
  4320387; US 4720860; US 4800590; WO 8806826; WO 8809541; EP 311112; US
  4509093; US 4578530; US 4599489; US 4731841; US 4802216; US 4819267; US
  4855062; US 4885778; US 4890323
Patent Details:
Patent No  Kind Lan Pg   Main IPC    Filing Notes
WO 9106926    A
   Designated States (National): AU CA JP
   Designated States (Regional): AT BE CH DE DK ES FR GB GR IT LU NL SE
US 5097505    A      12
EP 497889     A1 E  53 G07C-009/00   Based on patent WO 9106926
   Designated States (Regional): AT BE CH DE ES FR GB IT LI NL SE
JP 5503598    W        G06K-017/00   Based on patent WO 9106926
EP 555219     A1 E  22 H04K-001/00   Based on patent WO 9207436
   Designated States (Regional): BE CH DE DK ES FR GB IT LI NL SE
AU 642362     B        G07C-009/00   Previous Publ. patent AU 9067208
                                     Based on patent WO 9106926
JP 6507277    W      1 H04L-009/32   Based on patent WO 9207436
EP 497889     B1 E  23 G07C-009/00   Based on patent WO 9106926
   Designated States (Regional): AT BE CH DE ES FR GB IT LI NL SE
DE 69024367   E        G07C-009/00   Based on patent EP 497889
                                     Based on patent WO 9106926
ES 2084710    T3       G07C-009/00   Based on patent EP 497889
CA 2072150    C        G07C-009/00

Abstract (Basic): WO 9106926 A
```

The personal identification system has a unit to be carried by a person to be identified. The unit contains, memory for storing a predetermined coded **value** . A circuit **changes** a predetermined portion of the coded value at time intervals in accordance with a predetermined algorithm. The algorithm is such that the value of the portion of the stored coded value at any given time is nonpredictable. A circuit producing a triggering signal, and a second circuit responsive to the triggering signal causes an indication of the current stored coded value to be automatically produced in a predetermined sequence.

A station having circuiting automatically responsive to the produced coded value sequence identifies the person who is to be carrying the unit.

ADVANTAGE - Permits verification by proximity to checkpoint. (53pp Dwg.No.1/2

Abstract (Equivalent): EP 497889 B

The personal identification system has a unit to be carried by a person to be identified. The unit contains memory for storing a predetermined coded **value** . A circuit **changes** a predetermined portion of the coded value at time intervals in accordance with a predetermined algorithm. The algorithm is such that the value of the portion of the stored coded value at any given time is nonpredictable. A circuit producing a triggering signal, and a second circuit responsive to the triggering signal causes an indication of the current stored coded value to be automatically produced in a predetermined sequence.

A station having circuiting automatically responsive to the produced coded value sequence identifies the person who is to be carrying the unit.

ADVANTAGE - Permits verification by proximity to checkpoint.

(Dwg.1/2)

EP-555219 A device in the possession of an individual is used to generate a unique, time varying, non-predictable code. The code is mixed with a secret **PIN** for the individual. The mixed output is communicated to a central verification computer.

The computer typically strips the **PIN** from the communicated value, and uses the stripped **PIN** and remaining non-predictable code to perform a verification operation.

ADVANTAGE - Improved security against tapping of the line or obtaining possession of the user device.

(Dwg.1/3)

EP-497889 A personal identification system comprising: a unit (12) to be carried out by a person to be identified, said unit containing means (32) for storing a predetermined coded value, means (30) for changing at least a predetermined portion of the coded value at predetermined time intervals in accordance with a predetermined algorithm, the algorithm being such that the value of said predetermined portion of the stored coded value at any given time is nonpredictable, means (28,66,74) for producing a triggering signal, and means (30) responsive to said triggering signal for causing an indication of the current stored coded value to be automatically produced in a predetermined sequence; and a station (10) having means (48) automatically responsive to the produced coded value sequence for identifying the person who is to be carrying the unit, characterised in that said unit includes a keypad (36), and wherein said triggering signal producing means includes means responsive to a predetermined keypad input sequence for generating the triggering signal.

(Dwg.1/2

Abstract (Equivalent): US 5097505 A

Each person to be identified has a unit such as a card, badge or other taken or device which stores a predetermined coded value, a predetermined portion of which is changed at selected time intervals in accordance with an algorithm, the algorithm being such that the value of the predetermined portion of the stored coded value at any given time is nonpredictable. The unit has a triggering signal generator, the unit being responsive to the triggering signal to present an indication of the current sorted coded value to the station, the station responding to the predetermined coded value for identifying the person. Triggering may be in response to detection of a predetermined beacon from the station, in response to a user keypad input or may be periodically generated.

Security may be enhanced by the person inputting a unique **PIN** at the unit which **PIN** is utlized in generating the nonpredictable codes. The **PIN** input may also be used for triggering. Verification may be achieved by including a public code as part of the code which is presented from the unit which public code is not changed.

USE - Controlling passage into vault. (12pp)

US5168520 The appts. includes a unit for mixing the nonpredictable code generated by the device at a given time with the **PIN** according to a predetermined algorithm to generate a combined coded value. A modem separately communicates the nonsecret **identifying code** and the combined code value to the central verification computer.

The central verification computer includes a unit to use the nonsecret **identifying code** to retrieve the **PIN** and generate an appropriate, unique, time varying nonpredictable code for the individual, and a unit to use the retrieved **PIN** , appropriate nonpredictable code and the combined coded value in performing a verification operation.

ADVANTAGE - Improved security. **PIN** is never transmitted in uncoded form and is not resident in users appts. (card).

(Dwg.1/3

Title Terms: SYSTEM; SECURE; IDENTIFY; VERIFICATION; CODE; ACTIVE; UNIT; TIME; VARY; CODE; RESPOND; PROXIMITY; CHECKPOINT
Derwent Class: P76; Q47; T01; T05; W01; W02; W05; W06
International Patent Class (Main): G06K-017/00; G07C-009/00; H04K-001/00; **H04L-009/32**
International Patent Class (Additional): B01D-000/01; B01J-020/26; B42D-015/10; C02F-003/06; E05B-049/00; G06F-001/00; G06F-012/14; G06K-019/06; G07C-001/20; G07C-011/00
File Segment: EPI; EngPI
Manual Codes (EPI/S-X): T01-H01B; T01-X; T05-D; W02-G09; W05-B01A; W05-B01C ; W05-B01D; W05-D04; W05-D04A; W06-A04B

35/9/75 (Item 52 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

007813382
WPI Acc No: 1989-078494/198911
Related WPI Acc No: 1992-390280
XRPX Acc No: N89-059949

Identification and authentication system for computer security - has keyboard providing matrix of coefficients with numbers and letters to form password **for** encryption

Patent Assignee: COMPUTER SECURITY CORP (COMP-N)
Inventor: CAIRNS J P
Number of Countries: 009 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 306997	A	19890315	EP 88114858	A	19880912	198911	B

US 4962530	A	19901009	US 8795405	A	19870910	199043
CA 1320747	C	19930727	CA 577105	A	19880912	199336
EP 306997	B1	19941130	EP 88114858	A	19880912	199501
DE 3852253	G	19950112	DE 3852253	A	19880912	199507
			EP 88114858	A	19880912	
ES 2065903	T3	19950301	EP 88114858	A	19880912	199515

Priority Applications (No Type Date): US 8795405 A 19870910
Cited Patents: A3...8930; EP 147837; GB 2186106; No-SR.Pub; US 4034193; US 4184148; US 4333090; US 4502048
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 306997	A	E	22		
Designated States (Regional): DE ES FR GB IT NL SE					
EP 306997	B1	E	25	G07C-009/00	
Designated States (Regional): DE ES FR GB IT NL SE					
DE 3852253	G			G07C-009/00	Based on patent EP 306997
ES 2065903	T3			G07C-009/00	Based on patent EP 306997
CA 1320747	C			G06F-009/44	

Abstract (Basic): EP 306997 A

Inputting of a character into the system is initiated by actuation of one of nine contact switches (10A-10I) disposed in a three-by-three matrix. Variable visible indicia are shown on LEDs (30A-I) associated with respective keys. The symbols on the LEDs are subjects of the code alphabet from which the string of symbols for the **password** is selected. A string forming a **password** is made up of matrix coefficients and binary digits representing numbers and letters. The **password** is used for authenticating a user seeking access to a restricted resource by logging in the **password** .

The **numbers** and letters **change** in each display cycle which accompanies the logging-in of a symbol for identification ano authentication. A ROM (27) associated with the matrix stores the configuration of characters to be placed on the matrix at each oisplay cycle. The **encryption** ROM is programmed to respond to provide characters in successive display cycles.

ADVANTAGE - Prevents disclosure of code from observation of keyboard display

Abstract (Equivalent): EP 306997 B

A security apparatus for identification of preselected code of symbols comprising in combination an arrangement of a plurality of locations of manual switches (10A-1) said switches (10A-1) being selectively and sequentially actuatable to produce a sequence of values defining an actuated code of symbols, a first memory (X) means for providing pulses representing the actuated code of symbols upon actuation of said switches, means (35) associated with said first memory (X) for receiving the values of said actuated code of symbols, a microprocessor having a second memory (40) accessed by the microprocessor, means for storing in said second memory a preselected code of symbols, said microprocessor having means (37) for comparing the actuated code of symbols with the stored code of symbols, characterised in that said arrangement of a plurality of locations of manual switches is a matrix (33) consisting of an arrangement of a plurality of locations and matrix coefficients which are coordinate positions within the matrix defined by row and column, and including selectively operable manual switches and variable visible indicia associated with said switches, said indicia operative to display alphanumeric characters consisting of letters and numerals at said locations, said preselected code of symbols in the form of a digital binary coded decimal code consisting of alphanumeric characters and matrix coefficients, so that a matrix coefficient is a code value

represented by a visible indicia at a selected location at a selected sequence in said preselected code said first memory (X) containing said alphanumeric characters and matrix coefficients for display on said variable indicia, said means (35) associated with said first memory (X) displaying characters on said variable indicia, including the character contained in the preselected code of symbols if a character is to be inputted at this actuation step, said stored code in said second memory (40) consisting of at least one alphanumeric character and at least one matrix coefficient said microprocessor being operative to sequentially enter to said microprocessor pulses defining said actuated code of symbols which pulses represent the character displayed at the location of the actuated switch when the symbol to be entered at this step is a character, or represent the matrix coefficient corresponding to the position of the actuated switch independently of the character displayed at this location when the symbol to be entered at this step is a matrix coefficient, said compari

(Dwg.1/10b

)

Abstract (Equivalent): US 4962530 A

Each of the variable visible indicia is associated with a key. Upon each keystroke on the keyboard, the system randomly changes the positions of all of the indicia on the matrix. Because the true value of any particular key is independent of the value displayed on the variable visible indicia, a casual observer can not learn the keystrokes being entered into the keyboard.

If the code entered at the keyboard matches a stored value, the user is granted access. (20pp)

Title Terms: IDENTIFY; AUTHENTICITY; SYSTEM; COMPUTER; SECURE; KEYBOARD; MATRIX; COEFFICIENT; NUMBER; LETTER; FORM; **PASSWORD ; ENCRYPTION**

Derwent Class: T01; T05

International Patent Class (Main): G06F-009/44; G07C-009/00

International Patent Class (Additional): G06F-003/02; G06F-015/21

File Segment: EPI

Manual Codes (EPI/S-X): T01-H01C; T05-D

```
File   9:Business & Industry(R) Jul/1994-2004/Mar 24
         (c) 2004 Resp. DB Svcs.
File  16:Gale Group PROMT(R) 1990-2004/Mar 25
         (c) 2004 The Gale Group
File  47:Gale Group Magazine DB(TM) 1959-2004/Mar 25
         (c) 2004 The Gale group
File 148:Gale Group Trade & Industry DB 1976-2004/Mar 25
         (c)2004 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 275:Gale Group Computer DB(TM) 1983-2004/Mar 25
         (c) 2004 The Gale Group
File 570:Gale Group MARS(R) 1984-2004/Mar 25
         (c) 2004 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2004/Mar 25
         (c) 2004 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2004/Mar 25
         (c) 2004 The Gale Group
File 649:Gale Group Newswire ASAP(TM) 2004/Mar 24
         (c) 2004 The Gale Group

Set     Items   Description
S1     274780   PIN OR PINS OR PID OR PIDS OR UIN OR UINS
S2       7729   (SEQUENCE? ? OR SERIES)(1N)(NUMERIC? OR NUMBER? ? OR NUMER-
             AL? ? OR ALPHANUMERIC?)
S3     229134   PASSWORD? OR PASSCODE? OR PASSKEY? OR PASSNUMBER? OR PASSV-
             ALUE?
S4      20919   PASS()(WORD? ? OR KEY? ? OR CODE? ? OR NUMBER? ? OR VALUE?
             ? OR IDENTIFIER? OR ID OR SEQUENCE?)
S5     122202   (ID OR IDENTIFY? OR IDENTIFICATION? OR IDENTIFIE? ? OR AUT-
             HENTICAT? OR ACCESS OR AUTHORIZ? OR AUTHORIS?)()(CODE? ? OR N-
             UMBER? ? OR SEQUENCE)
S6          1   COENCYPHER? OR COENCIPHER? OR COCYPHER? OR COCIPHER? OR CO-
             ENCRYPT? OR COINCOD? OR COENCOD?
S7         55   CO()(ENCIPHER? OR ENCYPHER? OR ENCOD??? ? OR INCOD??? ? OR
             ENCRYPT?)
S8     471719   VARIABLE? ?
S9      14451   S8(3N)(ADD OR ADDS OR ADDED OR ADDING OR ADDITIONAL OR SUP-
             PLEMENT? OR EXTRA OR AUXILIAR? OR ANCILL? OR ANOTHER OR AUGME-
             NT?)
S10    115192   (PARAMETER? OR PARAMETRE? OR VALUE OR VALUES OR NUMBER? ? -
             OR NUMERIC? OR NUMERAL? OR ALPHANUMERIC?)(2N)(CHANGEAB? OR CH-
             ANG??? ? OR VARY? OR VARIE? ? OR INCONSTAN? OR INDETERMINAT?)
S11      5894   (PARAMETER? OR PARAMETRE? OR VALUE OR VALUES OR NUMBER? ? -
             OR NUMERIC? OR NUMERAL? OR ALPHANUMERIC?)(2N)(UNFIX?? ? OR DY-
             NAMIC?)
S12      3038   S10:S11(3N)(ADD OR ADDS OR ADDED OR ADDING OR ADDITIONAL OR
              SUPPLEMENT? OR EXTRA OR AUXILIAR? OR ANCILL? OR ANOTHER OR A-
              UGMENT?)
S13       104   S1:S5(S)(S6:S7 OR S9 OR S12)
S14      1628   S1:S5(S)S10:S11
S15      1659   (FURTHER OR SECOND OR PAIR?? ?)(1W)S8
S16         6   S1:S5(S)S15
S17        56   S14(S)(ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR ENCOD???? ? OR
              INCOD???? ?)
S18       163   S13 OR S16:S17
S19        44   S18/1999:2004
S20       119   S18 NOT S19
S21        85   RD (unique items)

 21/3,K/3     (Item 1 from file: 16)
```

DIALOG(R)File 16:Gale Group PROMT(R)

06048544 Supplier Number: 53635270 (USE FORMAT 7 FOR FULLTEXT)
Banking on-line.(Switzerland)
Studer-Walsh, Margaret
SwissWORLD, n6, p36(1)
Dec-Jan, 1998
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 704

... attempting to access via internet must punch in the contract number of the account, a **password** and an **additional number** that **changes** each time the programme is entered. This number is then scratched off a list provided...

21/3,K/9 (Item 7 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

04855456 Supplier Number: 47142262 (USE FORMAT 7 FOR FULLTEXT)
Printing Edge unites technologies
Holland, Tony
Packaging Week, p13
Feb 20, 1997
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 188

The system links production line speed pad printing of logos or colour designs with **additional variable** laser coding for different batch or **identification numbers** , in a unit that comprises a robotic loading and unloading feature.

Items drawn from a...

21/3,K/12 (Item 10 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

02861137 Supplier Number: 43853110 (USE FORMAT 7 FOR FULLTEXT)
BT N America rolls out 4 new network security features and services for users of its Global Data Network
Common Carrier Week, pN/A
May 24, 1993
Language: English Record Type: Fulltext
Document Type: Newsletter; Professional Trade
Word Count: 164

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...problem industry estimates costs $3 billion per year: (1) User identification and authentication. (2) Data **encryption** . (3) Customized security reports. (4) Specialized consulting services. New security elements were designed "in response...

...and unauthorized network access," BTNA said. User identification/authentication aspect replaces older method of reusable

password that allows access to protected information, it said. New method provides each user with credit-card-sized device with LCD front that displays "pseudo randomly generated 6-digit **number** " that automatically **changes** every 60 sec., BTNA said. To gain access to protected information, user enters secret personal **identification** **number** (**PIN**) followed by number currently displayed on LCD. Network then evaluates information to verify user's **PIN** and **access** **code** that should be displayed on LCD. If both numbers pass checks, access is allowed, BTNA...

21/3,K/13 (Item 11 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

02857777 Supplier Number: 43848001 (USE FORMAT 7 FOR FULLTEXT)
BT North America launches 4 new network security features and services
Communications Daily, pN/A
May 20, 1993
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 164

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...problem industry estimates costs $3 billion a year: (1) User identification and authentication. (2) Data **encryption** . (3) Customized security reports. (4) Specialized consulting services. New security elements were designed "in response...

...and unauthorized network access," BTNA said. User identification/authentication aspect replaces older method of reusable **password** that allows access to protected information, it said. New method provides each user with credit-card-sized device with LDC front that displays "pseudo randomly generated 6-digit **number** " that automatically **changes** every 60 sec., BTNA said. To gain access to protected information, user enters secret personal **identification** **number** (**PIN**) followed by number currently displayed on LCD. Network then evaluates information to verify user's **PIN** and **access** **code** that should be displayed on LCD. If both numbers pass checks, access is allowed, BTNA...

21/3,K/14 (Item 12 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

02725676 Supplier Number: 43645651 (USE FORMAT 7 FOR FULLTEXT)
FISCHER & PORTER INTRODUCES SINGLE LOOP CONTROLLER
News Release, p1
Feb 12, 1993
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 392

... Controller is for applications where one variable must automatically be maintained in definite proportion to **another** **variable** . The **PID** algorithm is executed to maintain a controlled line at a predetermined proportion to the uncontrolled...

21/3,K/24 (Item 7 from file: 47)
DIALOG(R)File 47:Gale Group Magazine DB(TM)
(c) 2004 The Gale group. All rts. reserv.

03780471 SUPPLIER NUMBER: 12341521 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Keep casual PC snoops at bay with batch security. (password batch file; Toolkit) (Tutorial)
Richardson, Ronny; Moore, Stephen
PC-Computing, v5, n7, p316(3)
July, 1992
DOCUMENT TYPE: Tutorial ISSN: 0899-1847 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 2052 LINE COUNT: 00146

... identically to the first section but look for different characters. If you want a longer **password** , **add** more environmental **variables** to the top of the batch file and add more of these sections.
Testing the...

21/3,K/26 (Item 9 from file: 47)
DIALOG(R)File 47:Gale Group Magazine DB(TM)
(c) 2004 The Gale group. All rts. reserv.

03627831 SUPPLIER NUMBER: 11548489 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Securing local government. (security systems) (includes related article)
Rogers, Donna
American City & County, v106, n11, p44(6)
Nov, 1991
CODEN: ACCOD ISSN: 0149-337X LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 2015 LINE COUNT: 00164

... the reader sends out an RF signal that causes the card to begin transmitting its **encoded number** . The cards' **varying** frequencies are detected and translated into an **ID number** by the host computer. Advantages to this technology are hands-free operation via a card...

21/3,K/27 (Item 10 from file: 47)
DIALOG(R)File 47:Gale Group Magazine DB(TM)
(c) 2004 The Gale group. All rts. reserv.

03478224 SUPPLIER NUMBER: 09635001 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Spider Systems Inc. Spider Analyzer 320 2.3. (Hardware Review) (one of five evaluations of LAN analyzers in 'Five LAN analyzers meet diverse needs') (evaluation)
Fratus, John; Graeff, Al; Preuss, Don
PC Week, v7, n47, p110(2)
Nov 26, 1990
DOCUMENT TYPE: evaluation ISSN: 0740-1604 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 690 LINE COUNT: 00055

... PC Week Labs used this ability to help test the other network analyzers.

A configuration **variable adds** a **password** for using the traffic generation and protocol decoding modes. This feature can provide some securrity...

```
 21/3,K/37     (Item 5 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

08840832     SUPPLIER NUMBER: 18398381    (USE FORMAT 7 OR 9 FOR FULL TEXT)
Tune in to telecommunications.
Risk Management, v43, n6, p44(1)
June, 1996
ISSN: 0035-5593      LANGUAGE: English      RECORD TYPE: Fulltext; Abstract
WORD COUNT:   953    LINE COUNT:  00081

...     which will soon be able to recognize the user's voice, and the
introduction of  dynamic   PIN   numbers  that constantly  change , The
good news from her perspective is that since the stakes are very, high,
solutions...
? t21/3,k/44-45,48,60

 21/3,K/44     (Item 12 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

07526099     SUPPLIER NUMBER: 16237356    (USE FORMAT 7 OR 9 FOR FULL TEXT)
How to get your employees back from the Internet. (Live Wire) (Column)
Gallagher, Sean
Government Computer News, v13, n18, p57(2)
August 15, 1994
DOCUMENT TYPE: Column      ISSN: 0738-4300      LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT:   756    LINE COUNT:  00056

...     Data Encryption Standard algorithm to create "sniffless" passwords.
Other systems require authentication with a generated  number , like Secure
 Dynamics  Inc.'s SecurID smart card system.
     These hardware solutions can get pretty expensive. You may...


 21/3,K/45     (Item 13 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

06785996     SUPPLIER NUMBER: 14431757    (USE FORMAT 7 OR 9 FOR FULL TEXT)
Security products abound, but is toll fraud too tough?
O'Shea, Dan
Telephony, v225, n9, p7(2)
August 30, 1993
ISSN: 0040-2656      LANGUAGE: ENGLISH      RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT:   810    LINE COUNT:  00067

...     identification card with an access number that changes ramdomly
every 60 seconds, end-to-end  encryption  of sensitive data, security
reports and security consulting services.
     Despite the offensive against telecom fraud...


 21/3,K/48     (Item 16 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

06464413     SUPPLIER NUMBER: 13765114    (USE FORMAT 7 OR 9 FOR FULL TEXT)
```

BT N. America (BTNA) rolled out 4 new network security features and services for users of its Global Data Network. (BT North America Inc.) (Telephony)
Communications Daily, v13, n97, p6(1)
May 20, 1993
ISSN: 0277-0679 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 179 LINE COUNT: 00015

TEXT:
...with credit-card-sized device with LDC front that displays "pseudo randomly generated 6-digit **number** " that automatically **changes** every 60 sec., BTNA said. To gain access to protected information, user enters secret personal **identification number** (**PIN**) followed by number currently displayed on LCD. Network then evaluates information to verify user's **PIN** and **access code** that should be displayed on LCD. If both numbers pass checks, access is allowed, BTNA...

21/3,K/60 (Item 1 from file: 160)
DIALOG(R)File 160:Gale Group PROMT(R)
(c) 1999 The Gale Group. All rts. reserv.

02421369
Enigma Logic Introduces Multiple-Mode Security Token for Hand-Held Authentication of Computer Users
News Release November 13, 1989 p. 1

...device that offers asynchronous and/or time- independent synchronous operation for the generation of dynamic **passwords** . The device is packaged in a credit-card plastic case that is one eighth of...

... The new card's operational paradigms can range from synchronous, single-stroke generation of dynamic **passwords** - based upon usage histories stored within the card's memory - to more formal challenge-response dialogues in which the card generates **encrypted passwords** in response to host-generated challenges. For additional security, the card can be configured with user- **changeable** personal **identification numbers** (**PIN** 's) that protect against unauthorilted use should a users card be lost or stolen. ...
? t21/3,k/61,64,69

21/3,K/61 (Item 2 from file: 160)
DIALOG(R)File 160:Gale Group PROMT(R)
(c) 1999 The Gale Group. All rts. reserv.

02270880
WESTINGHOUSE INTRODUCES TOKEN-BASED SECURITY SOFTWARE SYSTEM
News Release April 17, 1989 p. 1

... of security by requiring the validation of three separate items--a userid, a user-changeable **password** and a physical device (token). The introduction of NC-PASS represents Westinghouse Management Systems Software ...

...can be used with a variety of hardware tokens from any vendor supporting the Data **Encryption** Standard or a proprietary **encryption** algorithm. The tokens, electronic handheld devices, are used to generate a **dynamic numerical** code which is different each time the user attempts to access the system. Tokens vary from supplier to supplier. Some use a Personal **Identification Number** (**PIN**) or multiple **PINs** . **Encryption** algorithms may also generate time-synchronized **passwords** or utilize random challenge/response pairs. When a user attempts to log on using a...

21/3,K/64 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02112287 SUPPLIER NUMBER: 19905074 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Public key infrastructures. (protecting data within a network) (includes related article on whether to use outside certificate authorities) (Technology Information)
Karve, Anita
Network, v12, n12, p69(5)
Nov, 1997
LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 3953 LINE COUNT: 00307

... no one would be the wiser.

One way to get around this use of static **passwords** is to employ a two-factor token authentication system, such as that manufactured by Security...

...access the network by typing in a user name; however, instead of entering the same **password** each time, they carry a token that displays a **dynamic** string of **numerals** . These **changing** **numbers** are in sync with the network server, so as long as you enter the **password** the token displays for you before it changes, you're in. In other cases, information from a token is **encrypted** each time, ensuring a unique **password** for each login.

In most cases, these two-factor authentication systems are used almost exclusively...

21/3,K/69 (Item 6 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01704268 SUPPLIER NUMBER: 16255924 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Working with a net. (network security administration) (includes related article on network security)
Jacobs, Paula; Schwartz, Deborah
HP Professional, v8, n9, p42(6)
Sept, 1994
ISSN: 0896-145X LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 3162 LINE COUNT: 00263

... now a number of commercially available authentication types of products that can be used to **encrypt** sensitive, confidential data. They include Digital Pathways' (Mountain View, Calif.) Secure NetKey, a hand-held authentication calculator; Security Dynamics' (Cambridge, Mass.) Secure ID (complete turnkey systems), which provides a **changing** **number** authentication card; Racal-Guardata's (Herndon, Va.) WatchWord and WatchWord II, which provides an authentication calculator; and Enigma Logic's (Concord, Calif.) SafeWord, a card authentication calculator that supports onetime **passwords** .

Password protection is an area of major concern to network administrators. Guardian from DataLynx Inc...

```
File 696:DIALOG Telecom. Newsletters 1995-2004/Mar 24
         (c) 2004 The Dialog Corp.
File  15:ABI/Inform(R) 1971-2004/Mar 24
         (c) 2004 ProQuest Info&Learning
File  98:General Sci Abs/Full-Text 1984-2004/Feb
         (c) 2004 The HW Wilson Co.
File 484:Periodical Abs Plustext 1986-2004/Mar W3
         (c) 2004 ProQuest
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 635:Business Dateline(R) 1985-2004/Mar 24
         (c) 2004 ProQuest Info&Learning
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 369:New Scientist 1994-2004/Mar W2
         (c) 2004 Reed Business Information Ltd.
File 370:Science 1996-1999/Jul W3
         (c) 1999 AAAS
File  20:Dialog Global Reporter 1997-2004/Mar 25
         (c) 2004 The Dialog Corp.
File 624:McGraw-Hill Publications 1985-2004/Mar 24
         (c) 2004 McGraw-Hill Co. Inc
File 634:San Jose Mercury  Jun 1985-2004/Mar 24
         (c) 2004 San Jose Mercury News
File 647:CMP  Computer Fulltext 1988-2004/Mar W2
         (c) 2004 CMP Media, LLC
File 674:Computer News Fulltext 1989-2004/Mar W2
         (c) 2004 IDG Communications
File 621:Gale Group New Prod.Annou.(R) 1985-2004/Mar 25
         (c) 2004 The Gale Group

Set     Items   Description
S1     213844   PIN OR PINS OR PID OR PIDS OR UIN OR UINS
S2      11683   (SEQUENCE? ? OR SERIES)(1N)(NUMERIC? OR NUMBER? ? OR NUMER-
             AL? ? OR ALPHANUMERIC?)
S3     131580   PASSWORD? OR PASSCODE? OR PASSKEY? OR PASSNUMBER? OR PASSV-
             ALUE?
S4      15081   PASS()(WORD? ? OR KEY? ? OR CODE? ? OR NUMBER? ? OR VALUE?
             ? OR IDENTIFIER? OR ID OR SEQUENCE?)
S5      80823   (ID OR IDENTIFY? OR IDENTIFICATION? OR IDENTIFIE? ? OR AUT-
             HENTICAT? OR ACCESS OR AUTHORIZ? OR AUTHORIS?)()(CODE? ? OR N-
             UMBER? ? OR SEQUENCE)
S6          4   COENCYPHER? OR COENCIPHER? OR COCYPHER? OR COCIPHER? OR CO-
             ENCRYPT? OR COINCOD? OR COENCOD?
S7         21   CO()(ENCIPHER? OR ENCYPHER? OR ENCOD??? ? OR INCOD??? ? OR
             ENCRYPT?)
S8     415847   VARIABLE? ?
S9      15081   S8(3N)(ADD OR ADDS OR ADDED OR ADDING OR ADDITIONAL OR SUP-
             PLEMENT? OR EXTRA OR AUXILIAR? OR ANCILL? OR ANOTHER OR AUGME-
             NT?)
S10    113455   (PARAMETER? OR PARAMETRE? OR VALUE OR VALUES OR NUMBER? ? -
             OR NUMERIC? OR NUMERAL? OR ALPHANUMERIC?)(2N)(CHANGEAB? OR CH-
             ANG??? ? OR VARY? OR VARIE? ? OR INCONSTAN? OR INDETERMINAT?)
S11      4651   (PARAMETER? OR PARAMETRE? OR VALUE OR VALUES OR NUMBER? ? -
             OR NUMERIC? OR NUMERAL? OR ALPHANUMERIC?)(2N)(UNFIX?? ? OR DY-
             NAMIC?)
S12      2446   S10:S11(3N)(ADD OR ADDS OR ADDED OR ADDING OR ADDITIONAL OR
              SUPPLEMENT? OR EXTRA OR AUXILIAR? OR ANCILL? OR ANOTHER OR A-
             UGMENT?)
S13      2379   (FURTHER OR SECOND OR PAIR?? ?)(1W)S8
```

```
S14         54   S1:S5(S)(S6:S7 OR S9 OR S12)
S15       1103   S1:S5(S)S10:S11
S16          3   S1:S4(S)S13
S17         63   S15(S)(ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR ENCOD???? ? OR
               INCOD???? ?)
S18        118   S14 OR S16:S17
S19         71   S18/1999:2004
S20         47   S18 NOT S19
S21         40   RD (unique items)
```

21/3,K/3   (Item 2 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2004 ProQuest Info&Learning. All rts. reserv.

01650130 03-01120
Capture Information Once and Keep It
Spate, Joe
Manufacturing Systems v16n5 PP: 34-38 May 1998
ISSN: 0748-948X JRNL CODE: MFS
WORD COUNT: 1235

...TEXT: bottlenecks, it turned to Auto ID to help fill in the blanks. 2D symbologies, which **encode** all information in one label and collects data with one scan, provided previously lacking information for each pallet and container. Each 2D label **encodes** the supplier code, delivery order number, part **number** , quantity, engineering **change** level, **sequence number** , and advance ship notice (ASN) number.

In early 1997. the company began testing the program...

21/3,K/8   (Item 7 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2004 ProQuest Info&Learning. All rts. reserv.

01232786 98-82181
Tune in to telecommunications
Anonymous
Risk Management v43n6 PP: 44 Jun 1996
ISSN: 0035-5593 JRNL CODE: RMT
WORD COUNT: 884

...TEXT: various loss control and technological approaches to protect phone callers. The answers lie somewhere between **encryption** , velocity checking, radio frequency signatures, which will soon be able to recognize the user's voice, and the introduction or **dynamic PIN numbers** that constantly **change** . The good news from her perspective is that since the stakes are very high, solutions...

21/3,K/10   (Item 9 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2004 ProQuest Info&Learning. All rts. reserv.

01053355 97-02749
Secure communications
Kirch, John F
Security Management v39n6 PP: 17-19 Jun 1995
ISSN: 0145-9406 JRNL CODE: SEM
WORD COUNT: 788

...ABSTRACT: back office operations are centralized at the home office. The company installed the Access Control **Encryption** system, made by Security Dynamics Inc. Users are issued SecurID smart cards, which resemble credit ...

...display (LCD) window in the upper right hand corner. The window displays a 6-digit **number** that **changes** once every 60 seconds. To access the main computer system from a remote site, a user logs in the card's **PIN** number as well as the **passcode** shown in the LCD window at that moment.

21/3,K/13 (Item 12 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2004 ProQuest Info&Learning. All rts. reserv.

00959366 96-08759
Who's listening?
Betts, Mitch
Computerworld v29n1 PP: 66 Dec 26, 1994/Jan 2, 1995
ISSN: 0010-4841 JRNL CODE: COW
WORD COUNT: 491

...TEXT: a scanner.

But there's more. CDPD modems scramble the airborne data using public key **encryption** from RSA Data Security, Inc. in Redwood City, Calif. They also provide a frequently **changing identification number** for the user's device to thwart hackers who capture **ID numbers** .

On top of that, corporate network managers can add their own security measures, such as...

21/3,K/17 (Item 16 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2004 ProQuest Info&Learning. All rts. reserv.

00766516 94-15908
Security products abound, but is toll fraud too tough?
O Shea, Dan
Telephony v225n9 PP: 7, 13 Aug 30, 1993
ISSN: 0040-2656 JRNL CODE: TPH
WORD COUNT: 754

...TEXT: security services for its data customers. These services include a user identification card with an **access number** that **changes** randomly every 60 seconds, end-to-end **encryption** of sensitive data, security , reports and security consulting services.

Despite the offensive against telecom fraud...
? t21/3,k/27,31,37

21/3,K/27 (Item 1 from file: 624)
DIALOG(R)File 624:McGraw-Hill Publications
(c) 2004 McGraw-Hill Co. Inc. All rts. reserv.

0680408
BLOCKING THE INTERNAL THREAT: Authentication, Encryption, Single-Use Passwords and Internal Security

Open Computing July, 1995; Pg 48
Journal Code: UNIX ISSN: 0739-5922
Section Heading: IS IT NEGLIGENCES?
Word Count: 609 *Full text available in Formats 5, 7 and 9*

BYLINE:
R.K.

TEXT:
... keep coming. Hardware protection against theft of computer systems and mobile computers includes power-on **passwords** for access to the system and environment. Hard-drive security codes for mobile systems are similar to the personal **identification numbers** used in cellular telephones and actually prevent the hard drive from functioning until the right code number is entered. More sophisticated measures include single-use **passwords** and **changing** hardware **identification numbers** . Here is a select group of new **encryption** and authentication products:

AXENT TECHNOLOGIES, a division of Raxco Inc., offers several modules called OmniGuard...

21/3,K/31 (Item 4 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext
(c) 2004 CMP Media, LLC. All rts. reserv.

01052079 CMP ACCESSION NUMBER: cw19950508S0080
enterprise away team Telecommuting is great for businesses, but what's in store for network managers (letters to the editor)
DENISE PAPPALARDO
COMMUNICATIONSWEEK, 1995, n 556, PG43
PUBLICATION DATE: 950508
JOURNAL CODE: cw LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Closeup
WORD COUNT: 3095

... SecureID, a credit card- sized token.

The SecureID card has an LCD panel displaying a **number** that **changes** every 60 seconds. When a user dials into the ACE/Server machine's database, he or she is first asked for a personal **identification number** , then a **pass code** -the number on the LCD screen. This number is **encrypted** and sent to the ACE/Server machine over any LAN wire-even a phone line...

21/3,K/37 (Item 2 from file: 674)
DIALOG(R)File 674:Computer News Fulltext
(c) 2004 IDG Communications. All rts. reserv.

047493
Ready, set, GO REMOTE
NetworkWorld Review, NetworkWorld TEST ALLIANCE
In the race among six remote access servers, one unit takes the checkered flag.
Byline: Gerald Williams and Jonathan Torta
Journal: Network World Page Number: 41
Publication Date: October 16, 1995
Word Count: 2224 Line Count: 207

Text:
... Security Once users log on to a remote access server, they must still enter a **password** to gain access to other resources on the network. In addition, the network administrator can...

... Technologies, Inc. Secur-ID. With SecurID, end users get a smart card that displays an **identification number** that **changes** at a fixed interval, giving them unique **passwords** each time they log on. MAXserver 1620 also supports Kerberos, an authentication technique that uses a master host with **encrypted** logons. AccessBuilder 2000 provides broad support for third-party security packages. Routing tools Security features...
?

```
File   2:INSPEC 1969-2004/Mar W2
         (c) 2004 Institution of Electrical Engineers
File   6:NTIS 1964-2004/Mar W3
         (c) 2004 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1970-2004/Mar W1
         (c) 2004 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2004/Mar W2
         (c) 2004 Inst for Sci Info
File  35:Dissertation Abs Online 1861-2004/Feb
         (c) 2004 ProQuest Info&Learning
File  65:Inside Conferences 1993-2004/Mar W3
         (c) 2004 BLDSC all rts. reserv.
File  94:JICST-EPlus 1985-2004/Mar W2
         (c)2004 Japan Science and Tech Corp(JST)
File  95:TEME-Technology & Management 1989-2004/Mar W1
         (c) 2004 FIZ TECHNIK
File  99:Wilson Appl. Sci & Tech Abs 1983-2004/Feb
         (c) 2004 The HW Wilson Co.
File 111:TGG Natl.Newspaper Index(SM) 1979-2004/Mar 24
         (c) 2004 The Gale Group
File 144:Pascal 1973-2004/Mar W2
         (c) 2004 INIST/CNRS
File 202:Info. Sci. & Tech. Abs. 1966-2004/Feb 27
         (c) 2004 EBSCO Publishing
File 233:Internet & Personal Comp. Abs. 1981-2003/Sep
         (c) 2003 EBSCO Pub.
File 266:FEDRIP 2004/Feb
         Comp & dist by NTIS, Intl Copyright All Rights Res
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File 483:Newspaper Abs Daily 1986-2004/Mar 19
         (c) 2004 ProQuest Info&Learning
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group
File 603:Newspaper Abstracts 1984-1988
         (c)2001 ProQuest Info&Learning

Set     Items   Description
S1     134274   PIN OR PINS OR PID OR PIDS OR UIN OR UINS
S2      14086   (SEQUENCE? ? OR SERIES)(1N)(NUMERIC? OR NUMBER? ? OR NUMER-
             AL? ? OR ALPHANUMERIC?)
S3       9351   PASSWORD? OR PASSCODE? OR PASSKEY? OR PASSNUMBER? OR PASSV-
             ALUE?
S4        660   PASS()(WORD? ? OR KEY? ? OR CODE? ? OR NUMBER? ? OR VALUE?
             ? OR IDENTIFIER? OR ID OR SEQUENCE?)
S5      10998   (ID OR IDENTIFY? OR IDENTIFICATION? OR IDENTIFIE? ? OR AUT-
             HENTICAT? OR ACCESS OR AUTHORIZ? OR AUTHORIS?)()(CODE? ? OR N-
             UMBER? ? OR SEQUENCE)
S6          4   COENCYPHER? OR COENCIPHER? OR COCYPHER? OR COCIPHER? OR CO-
             ENCRYPT? OR COINCOD? OR COENCOD?
S7         11   CO()(ENCIPHER? OR ENCYPHER? OR ENCOD??? ? OR INCOD??? ? OR
             ENCRYPT?)
S8    1537137   VARIABLE? ?
S9      15131   S8(3N)(ADD OR ADDS OR ADDED OR ADDING OR ADDITIONAL OR SUP-
             PLEMENT? OR EXTRA OR AUXILIAR? OR ANCILL? OR ANOTHER OR AUGME-
             NT?)
S10    162012   (PARAMETER? OR PARAMETRE? OR VALUE OR VALUES OR NUMBER? ? -
             OR NUMERIC? OR NUMERAL? OR ALPHANUMERIC?)(2N)(CHANGEAB? OR CH-
             ANG??? ? OR VARY? OR VARIE? ? OR INCONSTAN? OR INDETERMINAT?)
S11     54314   (PARAMETER? OR PARAMETRE? OR VALUE OR VALUES OR NUMBER? ? -
             OR NUMERIC? OR NUMERAL? OR ALPHANUMERIC?)(2N)(UNFIX?? ? OR DY-
             NAMIC?)
S12      1020   S10:S11(3N)(ADD OR ADDS OR ADDED OR ADDING OR ADDITIONAL OR
              SUPPLEMENT? OR EXTRA OR AUXILIAR? OR ANCILL? OR ANOTHER OR A-
             UGMENT?)
S13        61   S1:S5 AND (S6:S7 OR S9 OR S12)
S14      1491   S1:S5 AND S10:S11
S15        14   S14 AND (ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR ENCOD???? ?
              OR INCOD???? ?)
S16          75   S13 OR S15
S17          31   S16/1999:2004
S18        2309   (FURTHER OR SECOND OR PAIR?? ?)(1W)S8
S19           7   S1:S5 AND S18
S20          82   S16 OR S19
S21          32   S20/1999:2004
S22          50   S20 NOT S21
S23          42   RD (unique items)
```

23/7/10 (Item 10 from file: 2)
DIALOG(R)File 2:INSPEC

02129391 INSPEC Abstract Number: B83056410
Title: Generation and reception of spread-spectrum signals
Author(s): Moser, R.
Author Affiliation: Locus Inc., Boalsburg, PA, USA
Journal: Microwave Journal vol.26, no.5 p.202-7
Publication Date: May 1983 Country of Publication: USA
CODEN: MCWJAD ISSN: 0026-2897
Language: English Document Type: Journal Paper (JP)
Treatment: Applications (A); General, Review (G)

Abstract: Discusses 'spread-spectrum' technique in which digitized information is added to a pseudo-random **number sequence** and the resultant bit stream **changes** some **parameter** of the carrier frequency in discrete increments. The rationale behind SS systems is to protect the signal from unwanted interference. The discrete modulation of the carrier frequency is usually performed either as a Multiple Level (M-ARY) Phase Shift Keyed (PSK) or Frequency Shift Keyed (FSK) Signal. The advent of ultra-complex monolithic integrated circuits is beginning to make spread-spectrum systems economical and available to the commercial field. (5 Refs)

Subfile: B

```
?t23/7/30
```

23/7/30 (Item 4 from file: 35)
DIALOG(R)File 35:Dissertation Abs Online

01352344 ORDER NO: AAD94-13339
THE IMPACT OF THE 1986 AND 1987 QUALIFIED PLAN REGULATION ON FIRMS' DECISION TO SWITCH FROM DEFINED BENEFIT TO DEFINED CONTRIBUTION FOR PLANS LARGER THAN 100 PARTICIPANTS
Author: BRADLEY, LINDA JACOBSEN
Degree: PH.D.
Year: 1993
Corporate Source/Institution: NORTH TEXAS STATE UNIVERSITY (0158)
Major Professor: CHARLES BOYNTON
Source: VOLUME 54/12-A OF DISSERTATION ABSTRACTS INTERNATIONAL.
PAGE 4503. 174 PAGES

Prior research has documented the trend since 1974 away from defined-benefit plans toward defined-contribution plans as the primary vehicle for employees' retirement income security. No published research has examined the specific impact of the four major legislative acts passed during 1986 and 1987 on this trend. The purpose of this research was to examine the United States population of plans with over 100 participants to determine the extent of the reaction away from defined benefit plans resulting from the 1986 and 1987 legislation.

This research organized the Internal Revenue Service form 5500 records into a time-series panel-data format covering the years 1984 through 1989 for each unique Employer **Identification Number** . The LIMDEP statistical computer package was used to formulate a pooled time-series, intervention-type, random-effects model. A separate multinomial logit regression on the population of defined-benefit plans existing in 1984 and 1985 predicted the probability of plan termination by 1990.

Prior research on the population of plans was achieved by performing cross-sectional regressions on selected years with explanatory variables including size of firm, one-digit SIC industry code, and union status. The present study is the first research of which the author is aware that examined the issue using a time-series approach tracking a specific firm through time. For the logit regression, **additional variables** unique to a plan (top heavy, integrated, maximum over/under funding, existence of a funding waiver request, change in retirement age) were examined.

Results indicated a decrease in defined-benefit (DB) coverage for 1986 and 1987 greater than expected, given the pre-existing downward trend. Size was positively correlated with the existence of a defined-benefit plan when addressing the entire population of firms reporting for any qualified plan. Surprisingly, size had minimal DB-plan-continuation prediction ability for firms with a pre-existing defined-benefit plan. Union existence and plan integration with Social Security appeared to exert a strong influence against DB plan termination.

?t23/7/42

23/7/42 (Item 1 from file: 233)

DIALOG(R)File 233:Internet & Personal Comp. Abs.

00372991 95MF01-018

Remotely Possible/Dial 4.0

Varhol, Peter D

Mobile Office , January 1, 1995 , v6 n1 p94-96, 2 Page(s)

ISSN: 1047-1952

Company Name: Avalan Technology

Product Name: Remotely Possible/Dial

Presents a favorable review of Remotely Possible/Dial v4.0 ($199), a remote control software from Avalan Technology of Holliston, MA (800, 508). Runs on IBM PC compatibles 25K to 50K of RAM, 1MB of hard disk space, a Hayes-compatible modem and Windows v3.1. Says that the product is one of the few packages designed entirely as a Windows application. Adds that it features a simple user interface, a toolbar. States that users can **change** modem **parameters** , **add** or modify **passwords** , or add items to the address book from the program's main menu. Also says that the installation process is fast and that it has high transfer rates. However, says that the program lacks on-line help. Concludes that the product provides remote access at excellent value. Includes a photo, a screen display and a summary card. (TLJ)

?

```
File 256:SoftBase:Reviews,Companies&Prods. 82-2004/Feb
         (c)2004 Info.Sources Inc

Set     Items   Description
S1        270   PIN OR PINS OR PID OR PIDS OR UIN OR UINS
S2         30   (SEQUENCE? ? OR SERIES)(1N)(NUMERIC? OR NUMBER? ? OR NUMER-
             AL? ? OR ALPHANUMERIC?)
S3       2075   PASSWORD? OR PASSCODE? OR PASSKEY? OR PASSNUMBER? OR PASSV-
             ALUE?
S4          5   PASS()(WORD? ? OR KEY? ? OR CODE? ? OR NUMBER? ? OR VALUE?
             ? OR IDENTIFIER? OR ID OR SEQUENCE?)
S5        262   (ID OR IDENTIFY? OR IDENTIFICATION? OR IDENTIFIE? ? OR AUT-
             HENTICAT? OR ACCESS OR AUTHORIZ? OR AUTHORIS?)()(CODE? ? OR N-
             UMBER? ? OR SEQUENCE)
S6          0   COENCYPHER? OR COENCIPHER? OR COCYPHER? OR COCIPHER? OR CO-
             ENCRYPT? OR COINCOD? OR COENCOD?
S7          0   CO()(ENCIPHER? OR ENCYPHER? OR ENCOD??? ? OR INCOD??? ? OR
             ENCRYPT?)
S8       1532   VARIABLE? ?
S9         35   S8(3N)(ADD OR ADDS OR ADDED OR ADDING OR ADDITIONAL OR SUP-
             PLEMENT? OR EXTRA OR AUXILIAR? OR ANCILL? OR ANOTHER OR AUGME-
             NT?)
S10       189   (PARAMETER? OR PARAMETRE? OR VALUE OR VALUES OR NUMBER? ? -
             OR NUMERIC? OR NUMERAL? OR ALPHANUMERIC?)(2N)(CHANGEAB? OR CH-
             ANG??? ? OR VARY? OR VARIE? ? OR INCONSTAN? OR INDETERMINAT?)
S11        20   (PARAMETER? OR PARAMETRE? OR VALUE OR VALUES OR NUMBER? ? -
             OR NUMERIC? OR NUMERAL? OR ALPHANUMERIC?)(2N)(UNFIX?? ? OR DY-
             NAMIC?)
S12         7   S10:S11(3N)(ADD OR ADDS OR ADDED OR ADDING OR ADDITIONAL OR
              SUPPLEMENT? OR EXTRA OR AUXILIAR? OR ANCILL? OR ANOTHER OR A-
             UGMENT?)
S13         0   S1:S5 AND (S6:S7 OR S9 OR S12)
S14         6   S1:S5 AND S10:S11
S15         0   (FURTHER OR SECOND OR PAIR?? ?)(1W)S8
S16         3   S14/1999:2004
S17         3   S14 NOT S16
?
```

```
File 347:JAPIO Nov 1976-2003/Nov(Updated 040308)
         (c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200419
         (c) 2004  Thomson Derwent
File 348:EUROPEAN PATENTS 1978-2004/Mar W02
         (c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20040318,UT=20040311
         (c) 2004 WIPO/Univentio

Set     Items   Description
S1         25   AU='GUNDLACH M':AU='GUNDLACH M R'
S2         23   AU='GUNDLACH MICHAEL':AU='GUNDLACH MICHAEL DR RER NAT'
S3         21   AU='NAUER B':AU='NAUER BERNHARD DIPL MATH'
S4          3   S1:S2 AND S3

 4/9/1     (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004  Thomson Derwent. All rts. reserv.

012712845    **Image available**
WPI Acc No: 1999-518958/199943
XRPX Acc No: N99-385927
  Service access protection method for telecommunication network - entering
  sequence of numbers by user and adding further parameter to sequence
  before transmission through network to central instance for evaluation
Patent Assignee: SIEMENS AG (SIEI  )
Inventor:  GUNDLACH M ;  NAUER B
Number of Countries: 021  Number of Patents: 004
Patent Family:
Patent No     Kind   Date     Applicat No    Kind   Date     Week
WO 9944332     A1  19990902  WO 98DE2949      A   19981002  199943  B
BR 9815697     A   20001114  BR 9815697       A   19981002  200064
                             WO 98DE2949      A   19981002
EP 1058982     A1  20001213  EP 98959711      A   19981002  200066
                             WO 98DE2949      A   19981002
JP 2002505552  W   20020219  WO 98DE2949      A   19981002  200216
                             JP 2000533979    A   19981002

Priority Applications (No Type Date): DE 1008523 A 19980227
Patent Details:
Patent No  Kind Lan Pg   Main IPC    Filing Notes
WO 9944332    A1 G  23 H04L-009/32
   Designated States (National): BR JP US
   Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU
   MC NL PT SE
BR 9815697    A        H04L-009/32   Based on patent WO 9944332
EP 1058982    A1 G     H04L-009/32   Based on patent WO 9944332
   Designated States (Regional): DE ES FR GB IT
JP 2002505552 W     19 H04L-009/32   Based on patent WO 9944332

Abstract (Basic): WO 9944332 A
        The method involves entering a number sequence which is only known
    by the user of the service. The number sequence is transmitted
    transparently in the communication network via exchange nodes (SSP) to
    a service control point (SCP) at which the number sequence is
    evaluated. The number sequence is supplemented by a changeable further
    parameter before the transmission through the communication network.
        The sequence is encoded using a mathematical algorithm. The result
    is transmitted to the service control point using multi-frequency
    dialling. An authentication is carried out in the service control
    point. Preferably, the telecommunication network is an intelligent
    network.
        USE - E.g. for credit card calling.
        ADVANTAGE - Provides better security against monitoring.
        Dwg.1/3
Title Terms: SERVICE; ACCESS; PROTECT; METHOD; TELECOMMUNICATION; NETWORK;
  ENTER; SEQUENCE; NUMBER; USER; ADD; PARAMETER; SEQUENCE; TRANSMISSION;
  THROUGH; NETWORK; CENTRAL; INSTANCE; EVALUATE
Derwent Class: P85; W01
International Patent Class (Main): H04L-009/32
International Patent Class (Additional): G06F-015/00; G09C-001/00;
  H04M-003/42; H04M-015/00
File Segment: EPI; EngPI
Manual Codes (EPI/S-X): W01-A05B; W01-B09; W01-C02A7A; W01-C02B6A; W01-C06;
  W01-C07A3; W01-C08F

 4/5/2     (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01084714
METHOD  AND DEVICE FOR SECURING ACCESS TO A SERVICE IN A TELECOMMUNICATIONS
    NETWORK
VERFAHREN  UND  VORRICHTUNG  ZUR  SICHERUNG  DES ZUGANGS ZU EINEM DIENST IN
    EINEM TELEKOMMUNIKATIONS-NETZ
PROCEDE  ET DISPOSITIF POUR LA SECURISATION DE L'ACCES A UN SERVICE DANS UN
    RESEAU DE TELECOMMUNICATION
PATENT ASSIGNEE:
  SIEMENS AKTIENGESELLSCHAFT, (200520), Wittelsbacherplatz 2, 80333 Munchen
    , (DE), (Applicant designated States: all)
INVENTOR:
   GUNDLACH, Michael , Vulpiusstrasse 87, D-81739 Munchen, (DE)
   NAUER, Bernhard , Fuggerstrasse 4, D-81373 Munchen, (DE
PATENT (CC, No, Kind, Date):  EP 1058982  A1  001213 (Basic)
                              WO 9944332  990902
APPLICATION (CC, No, Date):   EP 98959711 981002;  WO 98DE2949  981002
PRIORITY (CC, No, Date): DE 19808523 980227
DESIGNATED STATES: DE; ES; FR; GB; IT
INTERNATIONAL PATENT CLASS: H04L-009/32; H04M-015/00
CITED PATENTS (WO A): XP 2031268   ; XP 2031269
CITED REFERENCES (WO A):
  HOLLOWAY C J ET AL:  "EMPLOYING ONE-WAY FUNCTION METHODS FOR PIN
    VERIFICATION AND COMPOSITE KEY GENERATION IN ELECTRONIC FUNDS TRANSFER
    SYSTEMS" INTERNATIONAL DATA SECURITY CONFERENCE, 18. Februar 1985,
    Seiten 1-17, XP002031268
   "AUTHENTICATION WITH STORED KP AND DYNAMIC PAC. OCTOBER 1982" IBM
    TECHNICAL DISCLOSURE BULLETIN, Bd. 25, Nr. 5, Oktober 1982, Seiten
    2358-2360, XP002031269;
NOTE:
  No A-document published by EPO
LEGAL STATUS (Type, Pub Date, Kind, Text):
 Application:     001213 A1 Published application with search report
 Application:     991103 A1 International application. (Art. 158(1))
 Withdrawal:      031001 A1 Date application deemed withdrawn: 20030328
 Examination:     001213 A1 Date of request for examination: 20000628
 Examination:     021030 A1 Date of dispatch of the first examination
                            report: 20020917
 Application:     991103 A1 International application entering European
                            phase
LANGUAGE (Publication,Procedural,Application): German; German; German
```

4/5/3 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00512980 **Image available**
METHOD AND DEVICE FOR SECURING ACCESS TO A SERVICE IN A TELECOMMUNICATIONS NETWORK
PROCEDE ET DISPOSITIF POUR LA SECURISATION DE L'ACCES A UN SERVICE DANS UN RESEAU DE TELECOMMUNICATION

Patent Applicant/Assignee:
SIEMENS AKTIENGESELLSCHAFT,
GUNDLACH Michael,
NAUER Bernhard,
Inventor(s):
GUNDLACH Michael ,
NAUER Bernhard
Patent and Priority Information (Country, Number, Date):
Patent: WO 9944332 A1 19990902
Application: WO 98DE2949 19981002 (PCT/WO DE9802949)
Priority Application: DE 19808523 19980227
Designated States: BR JP US AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: H04L-009/32
International Patent Class: H04M-015/00
Publication Language: German
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 2599

English Abstract

The invention relates to a method for accessing a service in a telecommunications network, be it an intelligent network, a private network or a mobile radio network, from any kind of communications terminal. In order to gain access to the desired service, users must authenticate themselves by entering sequences of numbers. The invention also relates to a device in a telecommunications network for carrying out a secure authentication when a service is requested.